

Theory of Quantum System Certification

Martin Kliesch^{1,*} and Ingo Roth^{2,†}

¹*Quantum Technology Group, Heinrich Heine University Düsseldorf, Germany*

²*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, Germany*



(Received 14 September 2020; published 29 January 2021)

The precise control of complex quantum systems promises numerous technological applications including digital quantum computing. The complexity of such devices renders the certification of their correct functioning a challenge. To address this challenge, numerous methods were developed in the last decade. In this tutorial, we explain prominent protocols for certifying the physical layer of quantum devices described by quantum states and processes. Such protocols are particularly important in the development of near-term devices. Specifically, we discuss methods of direct quantum-state certification, direct-fidelity estimation, shadow-fidelity estimation, direct quantum-process certification, randomized benchmarking, and cross-entropy benchmarking. Moreover, we provide an introduction to powerful mathematical methods, which are widely used in quantum-information theory, in order to derive theoretical guarantees for the protocols.

DOI: [10.1103/PRXQuantum.2.010201](https://doi.org/10.1103/PRXQuantum.2.010201)

CONTENTS

I. INTRODUCTION	1	2. Schur-Weyl duality and the commutant of the diagonal action	25
A. Anatomy of quantum certification protocols	2	3. Uniformly random state vectors	27
B. Quantum certification for near-term devices—scalable certification of the physical layer	4	4. Unitary, spherical, and complex-projective k -designs	28
C. Structure and overview of the tutorial	4	J. Shadow-fidelity estimation	29
II. QUANTUM STATES	5	<i>Further reading</i>	31
A. Mathematical objects of quantum mechanics	5	III. QUANTUM PROCESSES	31
B. A definition of quantum-state certification	7	A. Quantum processes and measures of quality	32
C. Estimation and tail bounds	9	1. The Choi-Jamiołkowski isomorphism	32
D. Expectation value estimation for observables	11	2. Inner products of superoperators and fidelity measures	34
<i>Further reading</i>	12	3. The diamond norm	35
E. Distance measures for quantum states	12	B. Direct quantum-process certification	38
F. Direct quantum-state certification	14	<i>Further reading</i>	39
1. Stabilizer states	17	C. Randomized benchmarking	39
2. Extension towards fidelity estimation	18	<i>Interleaved randomized benchmarking</i>	42
<i>Further reading</i>	19	<i>Further reading</i>	43
G. Importance sampling	19	D. Cross-entropy benchmarking	44
H. Direct-fidelity estimation	20	<i>Cross-entropy and cross-entropy fidelity</i>	45
I. Random states and unitaries	23	<i>Cross-entropy benchmarking protocol</i>	46
1. Representation theory	24	<i>Further reading</i>	48
		ACKNOWLEDGMENTS	48
		ACRONYMS	49
		References	49

*info@mkliesch.eu

†i.roth@fu-berlin.de

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

I. INTRODUCTION

We are witnessing rapid progress in the experimental abilities to manipulate physical systems in their inner quantum properties such as state superposition and

entanglement. Most importantly, we begin to have precise control over complex quantum systems on scales that are out of reach of simulations on even the most powerful existing classical computing devices. Harnessing their computational power promises the development of digital quantum computers that solve important problems much faster than any classical computer. Envisioned applications also include, e.g., the study of complex phases of matter in analog simulations and cryptographically secure communication [1]. Hence, quantum technology promises highly useful devices with diverse domains of application ranging from fundamental research to commercial businesses.

With the advent of these novel technologies comes the necessity for certifying their correct functioning. The certification of quantum devices is a particularly daunting task in the interesting regime of high complexity as most straight-forward strategies based on classical simulations are bound to fail. Indeed, predicting the behavior of complex quantum devices quickly exhausts the available classical computing power. Ironically, it is the same complexity that makes quantum technology powerful that hinders their certification. This challenging perspective has already motivated extensive effort in developing certification tools for quantum devices in the last decades.

Intriguingly, numerous fields within the quantum sciences have tackled the problem of certification from a variety of different perspectives and have developed a large landscape of different protocols. These protocols operate under very distinct assumptions and resource requirements that are well motivated by the different perspectives. For example, certifying the correct function of a small-scale quantum device used in basic research allows one to invest sizeable effort. Here, one can potentially rely on a precise model of the physics of the device and might aim at a highly discriminative certificate providing plenty of information. A very different example is the certification of a server, correctly performing a quantum computation, by a remote client with standard desktop hardware. Such a protocol should be light weight on the client side and not rely on a detailed model of the server.

An attempt at a panoramic overview of the many approaches that all fall within the field of quantum certification was recently conducted in Ref. [2]. Therein, a very general classification framework for quantum certification protocols was proposed that is abstract enough to capture their wide range. Let us start by sketching the general framework. Thereby we can subsequently define the narrower scope of this tutorial.

A. Anatomy of quantum certification protocols

A *certification protocol* is a set of instructions that outputs either “accept” or “reject” concerning the

hypothesis that the device is functioning correctly, with a certain level of confidence.

The correct functioning of a device is defined in terms of a *measure of quality*. Such measures range from rigorous worst-case discrimination of “fundamental” physical objects modeling the device, to performance benchmarks defined in terms of tasks directly on the application layer. Note that in principle a measure of quality can be solely defined in terms of a protocol that can be reproducibly implemented. On the other hand, measures of quality that directly aim at the deviation of physical objects modeling the function of the device can provide an understanding of the device that is highly attractive in the development of the technology.

In this tutorial, we encounter a couple of such physically motivated measures of quality and study their mathematical properties and operational interpretations. These measures all map to the real line. Certification protocols then provide certificates that accept or reject the hypothesis of the measure of quality being smaller than a given ϵ . For this reason, most protocols that we present are *estimation protocols* for specific measures of quality that can be easily turned into ϵ -certification protocols by a standard method.

Theoretically, it is convenient to describe the protocol as involving three distinct objects, Fig. 1 (left). First, the *device* that is under scrutiny. Ideally, we try to be fairly conservative in the model and assumptions describing the device. Second, the protocol employs a *measurement apparatus*. The measurement apparatus, also a quantum device, is typically assumed to be much more precisely characterized compared to the device. Note that the device and measurement apparatus are not necessarily physically distinct devices. Choosing the split might be ambiguous and yield different formulation of the assumptions of the protocol. An extreme example are device-independent certification protocols that regard all quantum parts as a single device that is not subjected to any assumptions. In particular, they do not involve an anyhow characterized separate quantum measurement apparatus. The third object, is the *classical processor*, a classical computing device, that might take care of potentially required pre- and postprocessing tasks for the device control and the processing of the output data to arrive at a certificate or even communicates with the device and measurement apparatus in multiple rounds of an interactive protocol.

The landscape of protocols can be roughly organized according to three “axes.” The first axis comprises the set of *assumptions* that are imposed on the device and measurement apparatus to guarantee the functioning of the protocol.

A second axis summarizes the *complexity* of the resources that the protocol consumes. Each protocol requires a certain number of different measurement settings, its *measurement complexity*, that each require the

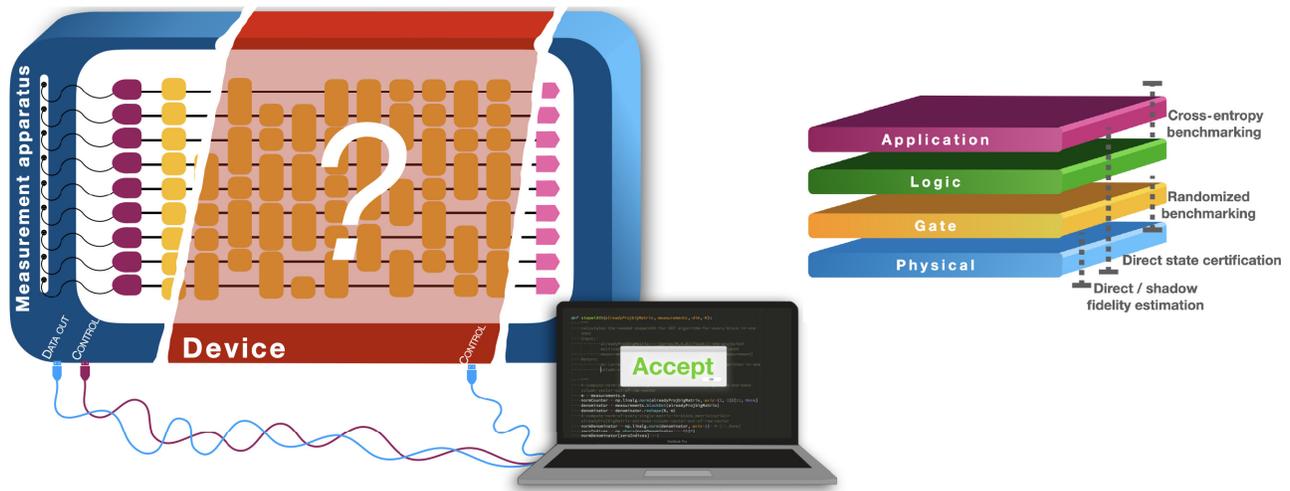


FIG. 1. Left: the theoretical description of protocols makes use of the distinction into the device, measurement apparatus, and classical processor. Right: a complex quantum device comprises multiple abstraction layers. Different protocols aim at certifying the functioning of the device on different layers. NISQ devices are not expected to feature a powerful logical-gate layer. Instead, applications are directly tailored to the physical-gate layer.

implementation of measurements that involve a certain *quantum measurement complexity*. To arrive at a final statistical estimate, a total number of repetitions of device invocations are required, the scaling of which is referred to as the *sample complexity*. Furthermore, as we already highlight at the beginning, a particularly important figure of merit for a protocol is that it comes with practically manageable demands in space and time for the classical processing tasks, its *classical processing complexity*. For our present scope, the mentioned complexity categories are the most important and are the focus of our discussion. Note, however, that this list is by far not complete, for example, interactive protocols might be compared in terms of challenging demands in the timing of the device's control.

The third and final axis is the *information gain* of the protocol. At a first glimpse this might come as a surprise as a protocol that outputs "accept" or "reject" might be regarded as always providing one bit of information. But different measures of quality have different discriminatory power among the hypothesis class that models the device compatible with the protocol's set of assumptions. For example, let us imagine a device preparing quantum states on demand. We might require the device to produce a quantum state that is ϵ -close in some distance measure to a specific target state. An alternative specification of the device might require it to always output the same quantum state but this quantum state should only be within a specified set of quantum states. In this situation, we can roughly say that the information gain restricting the device (within its allowed hypothesis class) is higher in the first specification compared to the latter one.

Concomitant with less information gain, it is conceivable that one can design a protocol for the latter specification with significantly less complexity compared to the first specification. Analysing the information gain in performing a certification task often allows one to derive lower bounds on the complexity of any protocol for this task. Beside the discriminatory power of the measure of quality, other intermediate steps in the certification protocol can reveal significantly more information about the device than is ultimately reflected in the measure of quality and the final certificate. For example, a potential certification protocol for our device that prepares quantum states might perform a high-precision, complete tomographic reconstruction of the quantum state and subsequently calculate the measure of quality using the tomographic estimate together with its error bounds. Conceptually, this example illustrates that certification is a subtask of the broader task of *quantum system characterization*, that encompasses protocols aiming at different types of information about a quantum system, e.g., identification of a quantum system or testing for a specific property. Protocols that perform quantum system identification or property estimation naturally also give rise to certification protocols. Note that in practice, the hidden information gain of a certification protocol can provide valuable information to calibrate and improve the device.

Another related task in *quantum system characterization* is the *benchmarking of quantum devices*. Benchmarking aims at comparing the performance of multiple devices. This can be done by comparing the achievable ϵ -value of ϵ -certificates of the respective devices. Benchmarking especially provides pragmatic impetus towards measures of quality that are not directly interpretable on the

physical layer. Instead, for the benchmarking of quantum devices it suffices to implicitly define a reproducible performance measure by specifying a protocol that returns the measure. The only required justification is that the measure is expected to be correlated with the performance in practically relevant tasks.

B. Quantum certification for near-term devices—scalable certification of the physical layer

For this tutorial, we select protocols that are particularly important for the certification of near-term quantum devices. Current and near-term quantum devices are still expected to be fairly noisy and of intermediate size, so-called noisy and intermediate scale quantum (NISQ) devices [3]. On the one hand, NISQ devices are in a regime of complexity where prominent certification methods that use full tomographic characterization become practically infeasible. On the other hand, there is still a large technological leap required in order to arrive at truly scalable devices, e.g., implementing fault-tolerant quantum computing. Such a full-fledged quantum device is described using multiple layers of abstraction from the physical layer over, e.g., physical- and logical-gate layers, to an application layer, see Fig. 1 (right). When a device already comes with multiple layers of abstraction one can also certify the functioning on the higher levels. NISQ devices, however, allow only for a bit of abstraction above the physical layer. For this reason, near-term quantum devices pose the need for certification techniques that aim at the physical layer but are scalable to the intermediate system sizes of NISQ devices. Such *scalable certification methods for the physical layer* are the focus of this tutorial.

In the long term, for complex quantum devices high-level certification on the application level, also referred to as *verification*, will become increasingly important. With cryptographic techniques quantum computations can be delegated to a remote server without revealing the actual computations. The correct execution of such *blind quantum computation* can be verified in different settings without many assumptions [4–8]. We do not cover these methods in this tutorial. Instead we refer to the review [9] of existing approaches for verifying quantum computations on devices that are close to being able to accurately perform a universal set of operations. Note that also on the long run, the scalable certification of the physical layer remains important for the diagnostic of the components of more complex quantum devices in the development and during run time.

We model the physical layer generically in terms of quantum states and processes throughout the tutorial. The model is general enough to capture different types of quantum devices used, e.g., in quantum-communication networks and analog simulators. Nonetheless, in this tutorial we take the certification of digital quantum-computing

devices as our main guiding problem. Particularly, the last two methods that we discuss, randomized benchmarking (RB) and cross-entropy benchmarking (XEB), are specifically designed for digital quantum-computing devices. RB aims at estimating the physical noise that compromises a gate layer. XEB aims at certifying the generation of samples from a probability distribution encoded in a quantum circuit. As such XEB can be regarded as a certification for the application layer of a digital quantum-computing device. But the application is deliberately designed very close to the physical layer.

In addition, we choose a set of protocols that can be presented and analyzed using a common set of mathematical methods. This allows us to combine our presentation of the certification protocol with a detailed introduction into the mathematical formalism that is required in order to prove rigorous performance guarantees for the protocols.

Lastly, we restrict our focus to certification protocols that employ measures of quality that are close to being natural measures of distance on the very fundamental physical description of the devices as quantum states and quantum processes. Also important and equally fundamental, but not captured in this tutorial, is the certification of specific properties such as entanglement or nonclassicality. Certain distinct properties, e.g., sufficiently high entanglement, allow for the certification of specific quantum states and processes even device independently. This class of so-called *self-testing protocols* is reviewed in Ref. [10].

One of the most intriguing aspects of the field of quantum certification is definitely the impressive stretch over multiple disciplines that come into play. Quantum certification is equally a field in applied mathematics, theoretical computer science, applied numerical computer science, experimental physics, and quantum hardware and software engineering. It comprises proofs of theorems, classical numerical studies of actual implementations, and performing the protocol in an actual quantum experiment including a diligent analysis of “real-world” data. Each of the disciplines involved comes with its own methods accustomed to the arising challenges. At the same time, looking at certification on different stages from theory to experiment holds valuable lessons that go in both directions. Having said this, we present a practically well motivated but theoretical formal framework for a set of quantum certification protocols. We do not delve into the exciting world of numerical and experimental implementations of the certification protocols that bring our model assumptions to the harsh scrutiny of “real-world” physics. Instead, practical considerations and desiderata constantly serve as our motivation and inform our discussion.

C. Structure and overview of the tutorial

The tutorial is split up in two major subsequent parts: the first part focusing on certification protocols for *quantum*

states, Sec. II, and the second part focusing on certification protocols for *quantum processes*, Sec. III. Furthermore, the tutorial consists of two different types of chapters: chapters that introduce the *mathematical preliminaries*, and chapters that present and analyze the *certification protocols*. We try to bring these two types of chapters in a dialog that goes back and forth between providing the motivation and tools for understanding the mathematical framework and protocols. The chapters on certification protocols conclude with suggestions for further reading on variants and extensions of the protocol and its theoretical analysis.

We highlight that the mathematical methods are core foundations of the broad field of theoretical quantum information and are by far not limited to quantum certification or even quantum characterization in their applications. Quite on the contrary, we expect the mathematical introductory chapters to serve as a valuable resource for students and researchers working on quantum information in general. At the same time experts in quantum information mainly interested in the presented certification methods might want to simply skip the mathematical introductory sections and focus on the protocols (Sec. II B, II D, II F, II H, II J, III B, III C, and III D).

In more detail, the mathematical methods and certification protocols presented here are the following: we start our discussion on quantum states with a brief introduction to the mathematical formalism of quantum mechanics, such as mathematical notions of operators and the modeling of quantum-mechanical measurements (Sec. II A). This allows us to formally introduce *quantum-state certification* as a one-sided statistical test in Sec. II B. Certification protocols rely on quantum-mechanical measurements, which are probabilistic in nature. Therefore, the confidence of the protocols is controlled using so-called *tail bounds* introduced in Sec. II C. As an example for an application of tail bounds, we derive the estimation error and the confidence when estimating *expectation values of observables* in Sec. II D. In order to *quantify* the accuracy of quantum-state preparations, we introduce relevant metrics on quantum states in Sec. II E. A popular metric is given by the (*Uhlmann*) *fidelity*. We provide a certification protocol in terms of the fidelity in Sec. II F. Stabilizer states are an important class of quantum states that can be certified with particularly few Pauli measurements (Sec. II F 1). Another approach to certification employs estimation protocols. Estimating the fidelity requires more measurements compared to the one-sided certification protocol. A tool to reduce the measurement effort is *importance sampling* introduced in Sec. II G. *Direct-fidelity estimation* uses this method to estimate the fidelity with respect to pure target states from relatively few state copies, Sec. II H.

For the remaining part of the tutorial random quantum states and random unitaries play an important role. For this reason, we introduce them in Sec. III. Certain random unitary operations allow, in general, for an estimation of

the fidelity from fewer state copies than direct-fidelity estimation, which we explain in Sec. II J on *shadow-fidelity estimation*.

We start our discussion of *quantum processes* with some mathematical preliminaries (Sec. III A), where we introduce the Choi-Jamiołkowski isomorphism (also known as channel-state duality), process fidelity measures quantifying average-case error measures and a worst-case error measure, the *diamond norm*. Most certification methods for quantum processes use average-case error measures. The presented quantum-state certification methods can be translated to quantum processes using the Choi-Jamiołkowski isomorphism. As an example, Sec. III B presents the resulting protocol for direct quantum-process certification. Such translated protocols, typically require high-quality state preparations and measurements to probe the quantum processes. A method tailored to quantum gates that allows the *average gate fidelity* to be extracted without requiring highly accurate state preparations and measurements is *randomized benchmarking* (Sec. III C). As our last protocol we discuss *cross-entropy benchmarking* in Sec. III D; this method has been used by Google to build trust in their recent experiment demonstrating the potential power of quantum computers in the task of generating certain random samples.

II. QUANTUM STATES

The first part of the tutorial is devoted to protocols that aim at certifying that a quantum state generated by a device is the correct one. We start by quickly reviewing and introducing the mathematical formalism of quantum mechanics. We expect that most of the presented material and the used basic mathematical notions are already known to the reader. Therefore, we are fairly brief in our presentation and aim at quickly setting up the notation that we use throughout the tutorial. For sake of completeness, we provide many details on the mathematical formalism. However, the main ideas behind the protocols and their theoretical guarantees can also be followed with a more superficial understanding of the mathematical preliminaries.

A. Mathematical objects of quantum mechanics

In order to discuss quantum states we set up some mathematical notation. We focus on finite-dimensional quantum mechanics in accordance with our emphasis on digital quantum computing. Hence, we assume all vector spaces to be finite dimensional. The space of *linear operators* from a vector space V to a vector space W is denoted by $L(V, W)$, and we set $L(V) := L(V, V)$. A *Hilbert space* is a vector space with an inner product $\langle \cdot, \cdot \rangle$. Let \mathcal{H} and \mathcal{K} be complex Hilbert spaces throughout the tutorial. We denote the *adjoint* of an operator $X \in L(\mathcal{H}, \mathcal{K})$ by X^\dagger , i.e., $\langle k, Xh \rangle = \langle X^\dagger k, h \rangle$ for all $h \in \mathcal{H}$ and $k \in \mathcal{K}$.

As customary in physics, we use the bra-ket notation (Dirac notation): we denote vectors by ket vectors $|\psi\rangle \in \mathcal{H}$ and linear functionals on \mathcal{H} by bra vectors $\langle\psi|$, which are elements of the dual space \mathcal{H}^* . Furthermore, we understand ket vectors and bra vectors with the same label as being related by the canonical isomorphism induced by the inner product. In bra-ket notation we frequently drop tensor-product operators to shorten the notation, e.g., $|\psi\rangle|\phi\rangle := |\psi\rangle \otimes |\phi\rangle \in \mathcal{K} \otimes \mathcal{H}$ or $|\psi\rangle\langle\psi| := |\psi\rangle \otimes \langle\psi| \in \mathcal{K} \otimes \mathcal{H}' \cong L(\mathcal{K}, \mathcal{H})$ for $|\psi\rangle \in \mathcal{K}$ and $|\phi\rangle \in \mathcal{H}$.

To describe the state of a quantum system we require the notion of *density operators*. The real subspace of *self-adjoint* operators, $X = X^\dagger$, is denoted by $\text{Herm}(\mathcal{H}) \subset L(\mathcal{H})$ and the convex cone of *positive semidefinite* operators by $\text{Pos}(\mathcal{H}) := \{X \in \text{Herm}(\mathcal{H}) \mid \langle\psi|X|\psi\rangle \geq 0\}$. The *trace* of an operator $X \in L(\mathcal{H})$ is $\text{Tr}[X] := \sum_i \langle i|X|i\rangle$, where $\{|i\rangle\} \subset \mathcal{H}$ is an arbitrary orthonormal basis of \mathcal{H} . The vector space $L(\mathcal{H})$ is itself a Hilbert space endowed with the Hilbert-Schmidt (trace) inner product

$$\langle X, Y \rangle := \text{Tr}[X^\dagger Y]. \quad (1)$$

The set of *density operators* is defined as $\mathcal{S}(\mathcal{H}) := \{\rho \in \text{Pos}(\mathcal{H}) : \text{Tr}[\rho] = 1\}$.

Outcomes of a quantum measurement are modeled by random variables. Abstractly, a *random variable* is defined as a measurable function from a probability space to a measurable space \mathcal{X} . Here, we are exclusively concerned with two types of random variable: (i) those that take values in a finite, discrete set $\mathcal{X} \cong [n] := \{1, \dots, n\}$ (understood as the measurable space with its power set as the σ -algebra) and (ii) those that take values in the reals $\mathcal{X} = \mathbb{R}$ (with the standard Borel σ -algebra generated by the open sets). In practice, the underlying probability space is often left implicit and one describes a random variable X taking values in \mathcal{X} directly by its probability distribution \mathbb{P} that assigns a probability to an element of the σ -algebra of \mathcal{X} . For example, for a random variable X taken values in \mathbb{R} and $I \subset \mathbb{R}$ an interval, we write $\mathbb{P}[X \in I]$ for the probability of X assuming a value in I . Abstractly speaking, \mathbb{P} is the push forward of the measure of the probability space to \mathcal{X} induced by the random variable X . Thus, \mathbb{P} is sufficient to describe X . The underlying probability space is, however, important to define correlations between multiple random variables, which are understood to be defined on the same probability space.

The probability distribution of a discrete random variable X taking values in a finite set $\mathcal{X} \cong [n]$ is characterized by its *probability mass function* $p_X : [n] \rightarrow [0, 1]$, $k \mapsto p_X(k) := \mathbb{P}[X = k] := \mathbb{P}(X \in \{k\})$. A real random variable X is characterized by its (*cumulative*) *probability distribution* $P_X : \mathbb{R} \rightarrow [0, 1]$, $x \mapsto P_X(x) := \mathbb{P}[X < x] := \mathbb{P}[X \in (-\infty, x)]$ or in case it is absolutely continuous by its *probability density* $p_X : \mathbb{R} \rightarrow [0, 1]$, $x \mapsto p_X(x) := dP_X(x)/dx$. Note that if a discrete random variable takes

values in a discrete subset of \mathbb{R} we can also assign a noncontinuous (cumulative) probability distribution.

The most general way to define a linear map from density operators $\mathcal{S}(\mathcal{H})$ to random variables is by means of a *positive operator-valued measure (POVM)*. A POVM is a map from (the σ -algebra) of \mathcal{X} to $\text{Pos}(\mathcal{H})$. For a discrete random variable X taking values in $[n]$ a POVM is uniquely defined by a set of *effects* $\{E_i \in \text{Pos}(\mathcal{H})\}_{i=1}^n$ with

$$\sum_{i=1}^n E_i = \mathbb{1}_{\mathcal{H}}, \quad (2)$$

where $\mathbb{1}_{\mathcal{H}} \in L(\mathcal{H})$ denotes the identity operator. Strictly speaking the POVM is the map on the power set of $[n]$ that extends $k \mapsto E_k$ additively. It is convenient and common to refer to the set of effects as the POVM. A POVM \mathbf{M} (with effects) $\{E_i \in \text{Pos}(\mathcal{H})\}_{i=1}^n$ induces a map from $\mathcal{S}(\mathcal{H})$ to random variables. To this end, we associate to ρ the random variable \mathbf{M}_ρ with probability mass function $p_{\mathbf{M}_\rho}(k) := \langle\rho, E_k\rangle$.

These are the ingredients to formalize the *static* postulates of quantum theory. We only require dynamics in Sec. III on quantum-process certification.

Postulate (quantum states and measurements):

- (i) Every quantum system is associated with a (separable) complex Hilbert space \mathcal{H} .
- (ii) The state of a quantum system, its *quantum state*, is described by a density operator $\rho \in \mathcal{S}(\mathcal{H})$.
- (iii) A *measurement* with potential outcomes in a finite, discrete set $O \cong [n]$ is described by a POVM \mathbf{M} with effects $\{E_i\}_{i \in [n]}$.
- (iv) If a quantum system is in the state $\rho \in \mathcal{S}(\mathcal{H})$ and the measurement \mathbf{M} is performed the observed outcome is a realization of the random variable \mathbf{M}_ρ associated to ρ by \mathbf{M} .

The set $\mathcal{S}(\mathcal{H})$ is convex. Its extremal points are rank-one operators. A quantum state $\rho \in \mathcal{S}(\mathcal{H})$ of unit rank is called a *pure* state. In particular, there exist a state vector $|\psi\rangle \in \mathcal{H}$ such that $\rho = |\psi\rangle\langle\psi|$. The state vector associated to a pure quantum state is only unique up to a phase factor. A general quantum state is therefore a convex combination of the form $\sum_i p_i |\psi_i\rangle\langle\psi_i|$, where p is a *probability vector*, i.e., an entry-wise non-negative vector $p \in \mathbb{R}^d$, $p \geq 0$ that is normalized, i.e., $\sum_i p_i = 1$. A quantum state that is not pure is called *mixed*.

Given two quantum systems, their joint system should also be a quantum system. This expectation is captured by the following postulate.

Postulate (composite quantum systems): The Hilbert space of two quantum systems with Hilbert spaces \mathcal{H}_1 and \mathcal{H}_2 , respectively, is the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$.

This construction induces an embedding from $L(\mathcal{H}_1)$ into $L(\mathcal{H}_1 \otimes \mathcal{H}_2)$ by

$$A \mapsto A \otimes \mathbb{1}. \quad (3)$$

Dually to that, for any state $\rho \in \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$

$$\text{Tr}[\rho(A \otimes \mathbb{1})] = \text{Tr}[\rho_1 A], \quad (4)$$

where ρ_1 is ρ reduced to system 1. The reduced state captures all information of ρ that can be obtained from measuring system 1 alone and can be explicitly obtained by the *partial trace* over the second subsystem

$$\begin{aligned} \text{Tr}_2 : L(\mathcal{H}_1 \otimes \mathcal{H}_2) &\rightarrow L(\mathcal{H}_1) \quad (\text{linear}) \\ X \otimes Y &\mapsto \text{Tr}_2[X \otimes Y] := X \text{Tr}[Y] \end{aligned} \quad (5)$$

as $\rho_1 := \text{Tr}_2[\rho]$.

By $\mathbb{F} \in L(\mathcal{H} \otimes \mathcal{H})$ we denote the *flip operator* (or *swap operator*) that is defined by linearly extending

$$\mathbb{F}|\psi\rangle|\phi\rangle := |\phi\rangle|\psi\rangle. \quad (6)$$

In a basis $\{|i\rangle\}_{i=1}^{\dim(\mathcal{H})}$ of \mathcal{H} , we can express $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ by a coefficient matrix $A \in \mathbb{C}^{\dim \mathcal{H} \times \dim \mathcal{H}}$ as $|\psi\rangle = \sum_{i,j} A_{ij} |i\rangle|j\rangle$. The coefficient matrix of $\mathbb{F}|\psi\rangle$ is given by the matrix transpose A^T of A with entries $(A^T)_{ij} = A_{j,i}$.

Lemma 1 (The swap trick): Let $\mathbb{F} \in L(\mathcal{H} \otimes \mathcal{H})$ be the *flip operator* from Eq. (6). For any $X \in L(\mathcal{H})$ it holds that

$$\text{Tr}[\mathbb{F}(X \otimes Y)] = \text{Tr}[XY]. \quad (7)$$

Proof. The identity can be checked by direct computation with basis elements or by using tensor network diagrams. We leave it as an exercise. ■

B. A definition of quantum-state certification

In this section, we define what we mean by a certification test for a quantum state. This definition will serve as the blueprint for the specific protocols that we present in the subsequent sections of the chapter. A state certification test solves the task of making sure that a quantum state prepared by a device $\tilde{\rho}$ is a sufficiently good approximation of a target state ρ . Due to the statistical nature of quantum measurements, the protocol for a certification test typically requires multiple copies of the quantum states. For this reason, it is appropriate to think of quantum-state certification as the certification of a device that repeatedly prepares a target state ρ .

In this tutorial we restrict our attention to single-round protocols, where a fixed number $n_{\tilde{\rho}}$ of copies of a target state is prepared and measured subsequently. Without further assumptions the output of the device is described

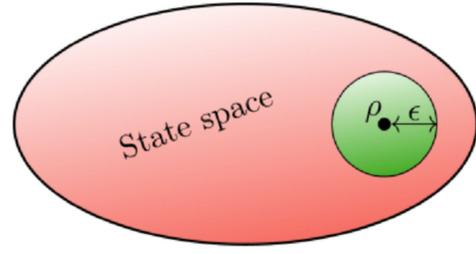


FIG. 2. The task of quantum-state certification is to detect when a state preparation $\tilde{\rho}$ is not close to a chosen target state ρ , i.e., when $\text{dist}(\rho, \tilde{\rho}) > \epsilon$.

by an output state $\tilde{\rho} \in \mathcal{S}[(\mathbb{C}^d)^{\otimes n_{\tilde{\rho}}}]$ on which the measurements are performed. Based on the measurement data the classical postprocessor then decides to accept or reject the hypothesis that the device prepared the target state within a specified accuracy.

This procedure is formalized by the notion of an ϵ -certification test, illustrated in Fig. 2. An ϵ -certification test should output “accept” if the prepared state is the targeted state in the majority of attempts. This requirement is referred to as *completeness*. Additionally, one demands an ϵ -certification to likely output “reject” in case the prepared state deviates from the target state beyond a tolerance. The deviation is quantified in terms of a distance measure on $\mathcal{S}(\mathbb{C}^d)$ taking values in \mathbb{R}_+ , the non-negative reals, and “beyond tolerance” means that it exceeds a certain *tolerated error threshold* $\epsilon > 0$. We arrive at the following definition for a single-round ϵ -certification test.

Definition 2 (Quantum-state ϵ -certification test): Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a quantum state, the *target state*, $\epsilon > 0$ and $\text{dist} : \mathcal{S}(\mathbb{C}^d) \times \mathcal{S}(\mathbb{C}^d) \rightarrow \mathbb{R}_+$ be a distance measure. An ϵ -certification test for ρ with respect to (w.r.t.) dist consists of a quantum measurement on the device output $\tilde{\rho} \in \mathcal{S}[(\mathbb{C}^d)^{\otimes n_{\tilde{\rho}}}]$ followed by classical postprocessing of the measurement data outputting either “accept” or “reject” and satisfying the *completeness* condition,

$$\tilde{\rho} = \rho^{\otimes n_{\tilde{\rho}}} \Rightarrow \mathbb{P}[\text{“accept”}] \geq \frac{2}{3}, \quad (8)$$

and the *soundness* condition holds for the reduced states $\tilde{\rho}_i$ of $\tilde{\rho}$,

$$\text{dist}(\rho, \tilde{\rho}_i) > \epsilon \forall i \in [n_{\tilde{\rho}}] \Rightarrow \mathbb{P}[\text{“reject”}] \geq \frac{2}{3}. \quad (9)$$

Note that more generally one could also define certification tests with respect to measures directly on the composite space $\mathcal{S}[(\mathbb{C}^d)^{\otimes n_{\tilde{\rho}}}]$.

The terms *completeness* and *soundness* are inspired by interactive proof systems. The role of these conditions can be clarified from the perspective of statistical hypothesis testing. In hypothesis testing one has a *null hypothesis* H_0

(usually the hypothesis that one hopes to disprove) and an *alternative hypothesis* H_1 and one needs to figure out which is true based on statistical data. In this setting, there are two types of error,

$$\mathbb{P}[\text{accept } H_1 \mid H_0] \quad (\text{type-I error}), \quad (10)$$

$$\mathbb{P}[\text{accept } H_0 \mid H_1] \quad (\text{type-II error}). \quad (11)$$

In state certification we choose null hypothesis H_0 to be “ $\text{dist}(\tilde{\rho}, \rho) > \epsilon$ ” and “ $\tilde{\rho} = \rho$ ” to be the alternative hypothesis H_1 . Then, for the output of the ϵ -state certification test $\mathbb{P}[\text{“reject”} \mid \tilde{\rho} = \rho]$ is the type-II error and $\mathbb{P}[\text{“accept”} \mid \text{dist}(\tilde{\rho}, \rho) > \epsilon]$ the type-I error. The completeness condition, Eq. (8), corresponds to requiring that the type-II error is bounded by $1/3$. Analogously, the soundness condition, Eq. (9), is the requirement that the type-I error is bounded by $1/3$.

For a test to meet the soundness and completeness condition additional assumptions on the prepared state $\tilde{\rho}$ can be required. A common assumption is that the device prepares a sequence of *independent* states. This means that

$$\tilde{\rho} = \tilde{\rho}_1 \otimes \tilde{\rho}_2 \otimes \cdots \otimes \tilde{\rho}_{n_{\tilde{\rho}}}, \quad (12)$$

with $\tilde{\rho}_i \in \mathcal{S}(\mathbb{C}^d)$ for all i . In principle, it is also conceivable that a device prepares entangled states to maliciously trick a certifier working under the independence assumption. But in many circumstances minimal control over the device or beliefs about its physically plausible limitations justify the independence assumptions.

An even stronger assumption is that the prepared states are *independent and identically distributed (i.i.d.)*. In this case, $\tilde{\rho} = \tilde{\rho}^{n_{\tilde{\rho}}}$. In the experimental practice it can be challenging to fulfill this assumption. For example, drifts in environmental parameters of a device can yield to a systematic deviation of the state copies that defy the i.i.d. assumption. Nonetheless, in many instances the i.i.d. assumption may be justified by a basic understanding of the functioning of the device and valid to a sufficient degree. In some situations, the i.i.d. assumption can be removed at the cost of a higher measurement effort using [11] a quantum de Finetti theorem [12] or an improved analysis [13,14].

The most important measures of complexity for an ϵ -certification test are the following.

Definition 3 (Sampling complexity): The *sample complexity* of a family of any such test $\{\mathcal{T}_{n_{\tilde{\rho}}}\}$ is (the scaling of) $n_{\tilde{\rho}}$ with d and ϵ .

The sampling complexity is the scaling of the number of states that the device needs to prepare for the test with the input parameters. In particular, in the context of digital quantum computing the statement that a “protocol is

efficient” is often understood as having sampling complexity in $O[\text{polylog}(d)]$ as this translates into a sampling complexity in $O[\text{poly}(n)]$ for a system of n qubits. Most guarantees that we prove for protocols in this tutorial, will consist in upper bounds on the sampling complexity of a test.

Another important measure for the practical feasibility of the protocol is the measurement complexity that quantifies how difficult it is to perform the quantum measurements of the protocol. In contrast to the precise definition of the sampling complexity, the measurement complexity should be regarded as a collection of different ways to formalize the demands of the measurement. For this reason, the discussion of the measurement complexity is of more qualitative nature.

In the context of state certification, an important aspect of measurement complexity is the number of copies that the POVM needs to act on simultaneously. The special case that encompasses all the presented protocols are *sequential measurements* where the measurements are only performed on the $n_{\tilde{\rho}}$ individual state copies separately. Therefore, the measurement device does not need to be able to store state copies before performing a measurement significantly lowering its complexity.

Another relaxation of the measurement complexity of sequential measurements are *nonadaptive measurements* where the performed measurement on an individual copy does not depend on the previously obtained measurement results. Furthermore, the complexity of the implementation of the POVM can be quantified, e.g., by measures for the complexity of the circuits required for its implementation in terms of local gates. The qualitative assessment of the measurement complexity as being experimentally feasible or not can vary widely for different devices and platforms.

A certification test is only required to accept the target state. However, in practice, such a test will accept states from some region around the target state with large probability. This property of a certification test is called *robustness (against deviations from the target states)*. One way of how such a robustness can be guaranteed is by estimating the distance of the targeted state ρ and the prepared state $\tilde{\rho}$, as we see in Sec. II H on *fidelity estimation*, which bounds on the distance. In this way, one obtains more information (a distance) than just certification (just “accept” or “reject”).

Clearly, one can also certify through full quantum-state tomography. However, the number of single sequential measurements in general required for tomography of a state $\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d)$ scales as $\Omega[d \text{rank}(\rho)]$ and as $\Omega[d^2 \text{rank}(\rho)^2]$ in the case two-outcome Pauli string measurements [15]. So, for the relevant case of pure n -qubit states this number scales at least as 2^n . This measurement effort becomes infeasible already for relatively moderate n .

In Sec. II H, we discuss that fidelity estimation can work with dramatically fewer measurements than full

tomography, when the target state has additional structure. In many situations, certification can work with even fewer measurements than fidelity estimation thanks to an improved ϵ -dependence in the sample complexity.

Our definition of a validation and certification test used the somewhat arbitrary confidence value of $2/3$. It is not hard to see that as long as the failure probability is bounded away from 1, the confidence can be amplified by repeating the test multiple times.

Proposition 4 (Confidence amplification): Let \mathcal{T}_{n_ρ} be an ϵ -certification test of a quantum state ρ from n_ρ i.i.d. samples with maximum failure probability $\delta = \frac{1}{3}$. We repeat the certification test N times and obtain a new certification test by performing a majority vote on the outcomes. Then the new test satisfies the *completeness* and *soundness* conditions

$$\sigma = \rho \Rightarrow \mathbb{P}[\text{"accept"}] \geq 1 - \delta, \quad (13)$$

$$\text{dist}(\rho, \tilde{\rho}) > \epsilon \Rightarrow \mathbb{P}[\text{"reject"}] \geq 1 - \delta, \quad (14)$$

for all $\sigma \in \mathcal{S}(\mathbb{C}^d)$, where $\delta = e^{-cN}$ and $c > 0$ is an absolute constant. The parameter $1 - \delta$ is also called the *confidence* of the test.

Proof. This statement can be checked directly from Definition 2. \blacksquare

We remark that the statement of this proposition also holds without the i.i.d. assumption. Here, only the proof of the soundness condition, Eq. (9), changes, since $\tilde{\rho}$ might be classically correlated or entangled across the $n_{\tilde{\rho}}$ subsystems. However, one can show (see, e.g., [16, Lemma 14.1] for the argument) that the worst case, given by a $\tilde{\rho}$ with minimum rejection probability, corresponds to a product state. This statement can be proven by choosing a basis for $(\mathbb{C}^d)^{\otimes n_{\tilde{\rho}}}$ for which the local measurements are all diagonal. Then the measurement outcomes only depend on the diagonal entries of $\tilde{\rho}$ and, hence, a worst case $\tilde{\rho}$ is a pure product state. This means that the worst case corresponds to i.i.d. state preparations.

Finally, we want to mention that, especially in the computer-science community, *certification* is often also called *verification*. In particular from an epistemological point of view, a physical model or hypothesis can never be fully verified. Therefore, we stick to the term *certification* for the physical layer where we actually model a device as being in a quantum state. This allows one to reserve the term *verification* to certification on higher level of device abstraction such as the application layer.

C. Estimation and tail bounds

A main technical tool for deriving the sampling complexity of certification protocols are tail bounds. The measurement outcomes of a quantum-mechanical experiment

are random variables. Recall that the expected value of a random variable X on a probability space (Ω, Σ, P) is defined as

$$\mathbb{E}[X] = \int_{\Omega} X(\omega) dP(\omega), \quad (15)$$

which gives rise to the well-known expressions

$$\mathbb{E}[X] = \sum_{k \in [n]} p_X(k) x_k \quad \text{and} \quad \mathbb{E}[X] = \int_{\mathbb{R}} x p_X(x) dx \quad (16)$$

for a discrete, finite random variable X taking values in $\{x_k\}_{k \in [n]}$ or a (absolutely continuous) real random variable X with p_X the probability mass function or probability density, respectively.

If we want to estimate a measure of quality, such as a distance measure for quantum states, we have to construct an estimator for that measure, which is a function of the measured outcomes. An estimator \hat{E} of a quantity E is itself a random variable (pushing forward the measure on the probability space). An estimator \hat{E} for E is said to be *unbiased* if $\mathbb{E}[\hat{E}] = E$. Our estimators will typically be families of random variables depending on a number of samples, i.e., the number of quantum states that the protocol consumes. In our notation we often leave this dependency implicit. We expect that if a protocol calculates an unbiased \hat{E} it reveals E accurately in the limit of infinite samples. Such an estimator is called *consistent*. To capture the effect of finite statistics, we introduce the notion of an ϵ -accurate estimator.

Definition 5 (ϵ -accurate estimator): Let $E \in \mathbb{R}$ and $\epsilon, \delta > 0$. A random variable \hat{E} taking values in \mathbb{R} is an ϵ -accurate estimator for E with confidence $1 - \delta$ if

$$\mathbb{P}[|\hat{E} - E| \leq \epsilon] \geq 1 - \delta. \quad (17)$$

The (scaling of) number of samples required for a family of estimators to be an ϵ -accurate estimator is its sampling complexity. The sampling complexity of estimators can be derived using *tail bounds* of random variables.

Tail bounds for random variables are bounds to the probability that a random variable assumes a value that deviates from the expected value, as visualized by the marked area in Fig. 3. Indeed, for any non-negative random variable X it is unlikely to assume values that are much larger than the expected value $\mathbb{E}[X]$:

Theorem 6 (Markov's inequality): Let X be a non-negative random variable and $t > 0$. Then

$$P_X(t) = \mathbb{P}[X \geq t] \leq \frac{\mathbb{E}[X]}{t}. \quad (18)$$

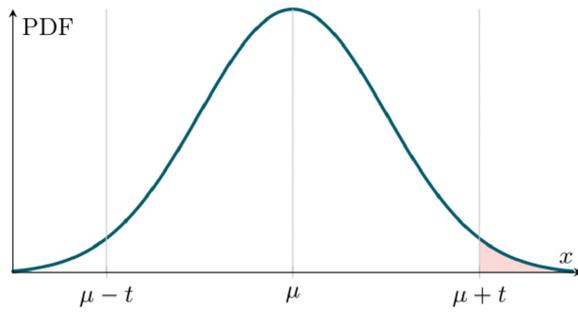


FIG. 3. The (upper) *tail* of a random variable X is the probability of X being greater than some threshold t . This probability is given by the corresponding area under the graph of the probability density function (PDF) of X .

Proof. Markov’s inequality is as elementary as its proof. Let (Ω, Σ, P) be the probability space of X . For the proof we denote the indicator function $\mathbf{1}_A$ of a subset $A \subset \Omega$ by

$$\mathbf{1}_A(x) := \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise.} \end{cases} \quad (19)$$

To prove Markov’s inequality we set $\{\omega : X(\omega) \geq t\}$ and observe that

$$t \mathbf{1}_{\{\omega : X(\omega) \geq t\}}(\omega') \leq X(\omega') \quad (20)$$

for all $\omega' \in \Omega$. Now taking the expected value of both sides of this inequality. ■

As a consequence of Markov’s inequality, the *variance* of a real random variable X ,

$$\text{Var}[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2, \quad (21)$$

can be used to control its tails.

Theorem 7 (Chebyshev’s inequality): Let X be a random variable, $\mathbb{E}[X] = 0$, with finite variance $\sigma^2 := \mathbb{E}[X^2]$. Then

$$\mathbb{P}[|X| \geq t] \leq \frac{\sigma^2}{t^2} \quad (22)$$

for all $t \geq 0$.

Proof. The proof follows by simply applying Markov’s inequality to the random variable X^2 . ■

Note that the assumption of mean zero is not really a restriction but only helps to state the theorem more concisely. In the case of a random variable Y that does not necessarily have a zero mean Chebyshev’s inequality yields a tail bound by applying it to $X := Y - \mathbb{E}[Y]$; see also Fig. 3. The same argument can be made for the tail bounds that follow.

A random variable X is called *bounded* if it takes values in a bounded subset of the reals almost surely. Its empirical mean is $(1/n) \sum_{i=1}^n X_i$, where $X_i \sim X$ are i.i.d. copies of X . In the case of bounded random variables, the empirical mean concentrates much more than a naive application of Markov’s or Chebyshev’s inequality suggests. More precisely, the following inequality holds (see, e.g., [17, Theorem 7.20]).

Theorem 8 (Hoeffding’s inequality): Let X_1, \dots, X_n be independent bounded random variables with $a_i \leq X_i \leq b_i$ almost surely for all $i \in [n]$ and denote their sum by $S_n := \sum_{i=1}^n X_i$. Then for all $t > 0$ it holds that

$$\mathbb{P}[S_n - \mathbb{E}(S_n) \geq t] \leq \exp \left[-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2} \right] \quad (23)$$

and

$$\mathbb{P}[|S_n - \mathbb{E}(S_n)| \geq t] \leq 2 \exp \left[-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2} \right]. \quad (24)$$

Proof. We only sketch the proof and recommend to flesh out the details as an exercise. The second statement directly follows from the first one. In order to prove the first one, let $s > 0$, apply Markov’s inequality to

$$\mathbb{P}[S_n - \mathbb{E}(S_n) \geq t] = \mathbb{P} \left\{ e^{s[S_n - \mathbb{E}(S_n)]} \geq e^{st} \right\}. \quad (25)$$

The independence of the X_i allows one to factorize the exponential and use the bounds on the range of X_i individually. Finally, choosing the optimal s yields the theorem’s statement. ■

Note that when one can additionally control the variance of bounded random variables then the Bernstein inequality [17, Corollary 7.31] can give a better concentration, especially for small values of t .

Another related tail bound is *Azuma’s inequality*, which allows for a relaxation on the independence assumption (supermartingales with bounded differences).

The *median of means estimator* is an estimator that allows for much better tail bounds than the empirical mean for the case of unbounded i.i.d. random variables with finite variance. The intuition is that taking the median of several empirical means is more robust against statistical outliers compared to taking the overall empirical mean.

Theorem 9 (Median of means estimator, version of [18, Theorem 2]): Let $\{X_i\}$ be i.i.d. random variables with mean μ and variance σ^2 and denote by $S_k := (1/k) \sum_{i=1}^k X_i$ the empirical mean from k i.i.d. samples. Take l empirical means $S_{k_j}, j \in [l]$, that are (i.i.d.) copies

of S_k and set

$$\hat{\mu} := \text{median}(S_{k,1}, \dots, S_{k,\ell}). \quad (26)$$

Then

$$\mathbb{P}\left[|\hat{\mu} - \mu| > \sigma\sqrt{4/\ell}\right] \leq e^{-k/8}. \quad (27)$$

In particular, for any $\delta \in (0, 1)$, $k = \lceil 8 \ln(1/\delta) \rceil$ and $m = k\ell$,

$$|\hat{\mu} - \mu| \leq \sigma\sqrt{\frac{32 \ln(1/\delta)}{m}} \quad (28)$$

with probability at least $1 - \delta$.

This theorem can be proven using Chebyshev's inequality for the empirical means $S_{k,j}$ and Hoeffding's inequality for a binomial distribution to obtain the concentration of the median. We refer to Ref. [18] for further details.

Finally, it is often required to bound the probability that at least one of several events is happening. For a series of events A_1, A_2, \dots the *union bound* (Boole's inequality) guarantees that

$$\mathbb{P}[A_1 \text{ or } A_2 \text{ or } \dots] \leq \sum_i \mathbb{P}[A_i]. \quad (29)$$

D. Expectation value estimation for observables

To familiarize ourselves with the application of tail bounds for the derivation of sampling complexities in quantum estimation, we turn our attention to a very basic task in quantum mechanics: the estimation of an expectation value of an observable.

We formulate a general quantum measurement in terms of a POVM. An important special case of a POVM is a *projector-valued measure (PVM)* where the effects are orthogonal projectors. A measurement described by a PVM is also called a *von Neumann/projective measurement*.

An *observable* quantity is modeled by a self-adjoint operator $A \in \text{Herm}(\mathcal{H})$. A self-adjoint operator has an eigendecomposition $A = \sum_{\alpha=1}^n a_\alpha P_\alpha$ with $a_\alpha \in \mathbb{R}$ and orthogonal projectors P_i onto the eigenspaces. The set of outcomes associated to the measurements of A is its real eigenvalue spectrum $\text{spec}(A) = \{a_\alpha\}_{\alpha \in [n]}$ and the measurement is described by the PVM that has the projectors P_α as effects. Thus, associated to an observable A is the map from $\mathcal{S}(\mathcal{H})$ to random variables $\rho \mapsto A_\rho$ taking values in $\text{spec}(A)$ with probability mass function $p_{A_\rho}(a_\alpha) = \text{Tr}[P_\alpha \rho]$. This implies that the expectation value of an observable $A \in \text{Herm}(\mathcal{H})$ in the state ρ is $\langle A \rangle_\rho := \mathbb{E}[A_\rho] = \text{Tr}[\rho A]$.

Given a quantum system in some state $\rho \in \mathcal{S}(\mathcal{H})$, we wish to estimate $\langle A \rangle_\rho$; note that the expectation value itself

cannot be observed directly but needs to be estimated from single measurements. One protocol for estimating $\langle A \rangle_\rho$ is to perform the projective measurement of the observable multiple times and use the observed empirical mean as an estimator for $\langle A \rangle_\rho$. Let $A_\rho^{(i)}$ be the random variable describing the outcome of the i th measurement of A in state ρ . The *empirical mean estimator* of m measurements is

$$Y^{(m)} := \frac{1}{m} \sum_{i=1}^m A_\rho^{(i)}. \quad (30)$$

It is easy to see that $Y^{(m)}$ is an unbiased estimator for $\langle A \rangle_\rho$. So how many copies of ρ does this protocol consume in order to arrive at an ϵ -accurate estimate of $\langle A \rangle_\rho$ with confidence $1 - \delta$?

If the measurements are independent and the eigenvalue spectrum of A is bounded, i.e., $a_\alpha \in [a, b]$ for all $\alpha \in [n]$, then Hoeffding's inequality, Eq. (24), yields a bound on the sampling complexity.

Proposition 10 (Estimation of observables): Let $\rho \in \mathcal{S}(\mathcal{H})$ and $A \in \text{Herm}(\mathcal{H})$ be an observable with $\text{spec}(A) \in [a, b]$. Choose $\epsilon > 0$ and $\delta \in (0, 1)$. The empirical mean estimator, Eq. (30), of the expectation value $\langle A \rangle_\rho$ from measurements of A on m independent copies of ρ satisfies

$$|Y^{(m)} - \langle A \rangle_\rho| \leq \epsilon \quad (31)$$

with probability at least $1 - \delta$ for all

$$m \geq m_0 = \frac{(b-a)^2}{2\epsilon^2} \ln \frac{2}{\delta}. \quad (32)$$

Proof. Having m independent state copies implies that the measurement outcomes are independent random variables. We choose X_1, \dots, X_m as independent copies of the random variable A_ρ/m . Then, the empirical mean estimator is described by a sum of m independent random variables $Y^{(m)} = \sum_{k=1}^m X_k$ with bounded range $X_k \in [a/m, b/m]$ for all k . Hoeffding's inequality yields

$$\mathbb{P}\left[|Y^{(m)} - \langle A \rangle_\rho| \geq \epsilon\right] \leq 2 \exp\left[-\frac{2m\epsilon^2}{(b-a)^2}\right] \quad (33)$$

for any $\epsilon > 0$. We wish this probability to be small, i.e., we require that

$$2 \exp\left[-\frac{2m\epsilon^2}{(b-a)^2}\right] \leq \delta \quad (34)$$

for some $\delta \in (0, 1)$ and determine the critical value m_0 required for the estimation by solving the inequality for $m = m_0$, which yields Eq. (32). ■

Proposition 10 guarantees that expectation values of bounded observables can be estimated with a measurement

effort that is independent of the Hilbert space dimension. The confidence $1 - \delta$ can be improved exponentially fast by increasing the measurement effort m .

One can define distance measures on $\mathcal{S}(\mathcal{H})$ in terms of expectation values of a set of observables. Naturally, the estimation protocol described in this section gives rise to an ϵ -certification test w.r.t. such measures.

Further reading

Using the union bound, one can easily generalize Proposition 10 to derive the sampling complexity of estimating multiple observables. The total number of sufficient state copies ρ to estimate ℓ different observables then scales as $m_0 \in O[\ell \log(2\ell/\delta)/\epsilon^2]$. In this setting each observable is estimated from a different measurement setting. In contrast, *Shadow estimation* [19–21] provides a way to estimate multiple observables from a single measurement setting. For certain types of observables, the shadow estimation has sampling complexity of $m_0 \in O[\ln(2\ell/\delta)/\epsilon^2]$ [21].

We further discuss shadow-estimation techniques in the context of state certification in Sec. II J.

E. Distance measures for quantum states

In our general definition of an ϵ -certification test, Definition 2, requires a distance measure on $\mathcal{S}(\mathcal{H})$. In this section we introduce some “natural” measures on quantum states.

To this end, recall that any *normal* operator $X \in L(\mathcal{H})$, i.e., any operator that commutes with its adjoint, $[X, X^\dagger] := XX^\dagger - X^\dagger X = 0$, can be written in spectral composition $X = \sum_i x_i P_i$, where $x_i \in \mathbb{C}$ are its eigenvalues and $P_j = P_j^2 \in Pos(\mathcal{H})$ the corresponding spectral projectors. There are several useful norms of an operator $X \in L(\mathcal{H}, \mathcal{K})$. For any operator $X \in L(\mathcal{H}, \mathcal{K})$ between two Hilbert spaces \mathcal{H} and \mathcal{K} , the operator $X^\dagger X$ is positive semidefinite, i.e., in $Pos(\mathcal{H})$. In consequence, it has a positive semidefinite square root $|X| := \sqrt{X^\dagger X} \in Pos(\mathcal{H})$.

The *spectral norm* (also known as operator norm) $\|X\|_{\text{op}} \in \mathbb{R}_+$ of X is defined to be the largest eigenvalue of $|X|$. The *trace norm* is $\|X\|_1 := \text{Tr}[|X|]$ and the *Frobenius norm* $\|X\|_F := \sqrt{\text{Tr}[|X|^2]} = \sqrt{\text{Tr}[X^\dagger X]}$. These norms can be defined in a variety of equivalent ways: the spectral norm coincides with the norm induced by the ℓ_2 -norm on \mathcal{H} via $\|X\|_{\text{op}} = \sup_{\|v\|_{\ell_2} \leq 1} \|Xv\|_{\ell_2}$, a manifestation of the Rayleigh principle. The Frobenius norm is induced by the *Hilbert-Schmidt inner product*, Eq. (1). It can also be expressed in terms of the matrix representation of X as $\|X\|_F = \sum_{i,j} |X_{ij}|^2$. Finally, all three norms are instances of the *Schatten p -norms* that are directly defined as ℓ_p -norms on the singular value spectrum. The singular value spectrum $\sigma(X)$ of X is defined as the eigenvalue spectrum of $|X|$ and the ℓ_p -norms are given by $\|x\|_{\ell_p} :=$

$(\sum_i |x_i|^p)^{1/p}$. This gives rise to the unitarily invariant Schatten p -norm $\|X\|_p := \|\sigma(X)\|_{\ell_p}$ and $\|\cdot\|_{\text{op}}$, $\|\cdot\|_1$, and $\|\cdot\|_F$ are the Schatten p -norms with $p = \infty, 1, 2$, respectively.

The Euclidean inner product is bounded by ℓ_p -norms by the Hölder inequality that states that for all $x, y \in \mathbb{C}^d$ and pairs $p, q \in \{1, 2, \dots, \infty\}$ with $p^{-1} + q^{-1} = 1$ (understanding $1/\infty = 0$) it holds that

$$|\langle x, y \rangle| \leq \|x\|_{\ell_p} \|y\|_{\ell_q}. \quad (35)$$

The Hölder inequality generalizes the Cauchy-Schwarz inequality, where $p = q = 2$. The Schatten p -norms inherit a *matrix Hölder inequality* from the Hölder inequality: let $X, Y \in L(\mathcal{H}, \mathcal{K})$ and p, q as before, then

$$|\langle X, Y \rangle| \leq \|X^\dagger Y\|_1 \leq \|X\|_p \|Y\|_q. \quad (36)$$

The Hölder inequality directly follows from the von Neumann inequality $\text{Tr}|AB| \leq \langle \sigma(A), \sigma(B) \rangle$, where the singular value spectra $\sigma(A)$ and $\sigma(B)$ are each descending [22]. Furthermore, the Schatten p -norms inherit the ordering of the ℓ_p -norms, $\|X\|_\infty \leq \dots \leq \|X\|_2 \leq \dots \leq \|X\|_1$ for all X . Norm bounds in reversed order will in general introduce dimensional factors. For low-rank matrices these bounds can be tightened.

Lemma 11 (Reversed norm bounds): For all $X \in L(\mathcal{H}, \mathcal{K})$ it holds that

$$\|X\|_1 \leq \sqrt{\text{rank}(X)} \|X\|_F \leq \text{rank}(X) \|X\|_{\text{op}}. \quad (37)$$

Proof. Let $X \in L(\mathcal{H}, \mathcal{K})$ and $r = \text{rank}(X)$. We can always write $X = XP_r$ with P_r a rank- r projector onto the orthogonal complement of the kernel of X . Now by the matrix Hölder inequality, Eq. (36), $\|X\|_1 = \|XP_r\|_1 \leq \|P_r\|_F \|X\|_F = \sqrt{r} \|X\|_F$. For the second inequality, bound again using the matrix Hölder inequality $|\text{Tr}[X^\dagger X]| \leq \|X^\dagger X\|_1 \leq \|P_r\|_1 \|X^\dagger X\|_{\text{op}} = r \|X\|_{\text{op}}^2$. Taking the square root we conclude that $\|X\|_F \leq \sqrt{r} \|X\|_{\text{op}}$ from which the second inequality follows. ■

A natural metric on quantum states is the *trace-distance* $\text{dist}_{\text{Tr}} : \mathcal{S}(\mathcal{H}) \times \mathcal{S}(\mathcal{H}) \rightarrow \mathbb{R}_+$,

$$\text{dist}_{\text{Tr}}(\tilde{\rho}, \rho) = \frac{1}{2} \|\rho - \tilde{\rho}\|_1. \quad (38)$$

We have already seen that compared to the other Schatten p -norms the trace norm is the largest, i.e., the most “pes-simistic” distance measure. Furthermore, the trace norm has an operational interpretation in terms of the distinguishability of quantum states by dichotomic measurements.

Proposition 12: (Operational interpretation of the trace distance): Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. It holds that

$$\text{dist}_{Tr}(\rho, \sigma) = \sup_{0 \leq P \leq \mathbb{1}} \text{Tr}[P(\rho - \sigma)]. \quad (39)$$

Furthermore, the supremum is attained for the orthogonal projector P^+ onto the positive part of $\rho - \sigma$.

Proof. First we show that the supremum is attained for P^+ . The self-adjoint operator difference can be decomposed as

$$\rho - \sigma = X^+ - X^- \quad (40)$$

into a *positive part* $X^+ \in \text{Pos}(\mathcal{H})$ and a *negative part* $X^- \in \text{Pos}(\mathcal{H})$. We note that $\|X^\pm\|_{\text{op}} \leq 1$. Since $\text{Tr}[X^+ - X^-] = \text{Tr}[\rho - \sigma] = \text{Tr}[\rho] - \text{Tr}[\sigma] = 0$, we have $\text{Tr}[X^+] = \text{Tr}[X^-]$. Moreover, $\|\rho - \sigma\|_1 = \text{Tr}[X^+] + \text{Tr}[X^-]$. The last two statements together yield that the trace distance between the two states is

$$\frac{1}{2} \|\rho - \sigma\|_1 = \text{Tr}[X^+] = \text{Tr}[P^+(\rho - \sigma)], \quad (41)$$

where P^+ is the orthogonal projector onto the support of X^+ . It can be calculated by means of the singular value decomposition of $\rho - \sigma = U\Sigma V^\dagger$ as $P^+ = U_+ V_+^\dagger$ with U_+ and V_+ the matrices with singular left and right vectors, respectively, associated to the positive singular values as its columns.

In order to show that the supremum cannot become larger than the trace distance, we consider some operator P with $0 \leq P \leq \mathbb{1}$. Then, indeed,

$$\begin{aligned} \text{Tr}[P(\rho - \sigma)] &= \text{Tr}[PX^+] - \text{Tr}[PX^-] \leq \text{Tr}[PX^+] \\ &\leq \|X^+\|_1 = \frac{1}{2} \|\rho - \sigma\|_1, \end{aligned} \quad (42)$$

where we use the matrix Hölder inequality, Eqs. (36) and (41), in the last two steps. ■

Given two quantum states the optimal dichotomic POVM measurement $\{P, \mathbb{1} - P\}$ to distinguish the two states is the POVM that maximizes the probability of measuring the outcome associated to P in one state and minimizes the same probability for the other state. Of course exchanging the role of P and $\mathbb{1} - P$ works equivalently. We can think of the achievable differences in probabilities as a measure for the distinguishability of ρ and σ . Proposition 12 shows that the trace distance of two states coincides with the maximal distinguishability by any dichotomic POVM measurements. This distinguishability of a single-shot measurement can be amplified by measuring multiple i.i.d. copies of a quantum state with $\{P, \mathbb{1} - P\}$. We turn this insight into an ϵ -certification test for pure states in the next section.

Before we do this, let us introduce another important distance measure on quantum states. The (*squared*) *fidelity* of two quantum state $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ is defined as

$$F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2. \quad (43)$$

Note that

$$\|\sqrt{\rho}\sqrt{\sigma}\|_1 = \text{Tr} \left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right]. \quad (44)$$

While not any more directly evident from Eq. (44), the fidelity is symmetric as is apparent from Eq. (43).

Some authors define the fidelity as $\|\sqrt{\rho}\sqrt{\sigma}\|_1$ without the square. For this reason, one might want to refer to the expression of Eq. (43) explicitly as the squared fidelity to avoid confusion. For brevity, we however call F simply the fidelity hereinafter.

The fidelity is more precisely not a measure of “distance” for two quantum states but of “closeness.” In particular, $F(\rho, \rho) = 1$, which can be seen to be the maximal values of $F(\rho, \sigma)$ for all $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. Hence, $0 \leq F(\rho, \sigma) \leq 1$ on $\mathcal{S}(\mathcal{H})$. Often it is convenient to work with the *infidelity* $1 - F(\rho, \sigma)$ as the complementary measure of “distance.”

When at least one of the states ρ or σ is pure, say $\rho = |\psi\rangle\langle\psi|$ then

$$F(\rho, \sigma) = \langle\psi|\sigma|\psi\rangle = \text{Tr}[\rho\sigma] = \langle\rho, \sigma\rangle, \quad (45)$$

which can easily be proven using Eq. (44). Furthermore, for both states being pure we have $F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle|^2$ for all $|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi| \in \mathcal{S}(\mathcal{H})$. Thus, for pure states the fidelity is the overlap of the states and can be related to the angle between the state vectors. We in fact mostly encounter the case where at least one of the states is pure and mostly work with Eq. (45) instead of Eq. (43).

The fidelity is related to the trace distance as follows.

Proposition 13: (Fuchs-van de Graaf inequalities [23, Theorem 1]): For any states $\rho, \sigma \in \mathcal{S}(\mathcal{H})$

$$1 - \sqrt{F(\rho, \sigma)} \leq \frac{1}{2} \|\rho - \sigma\|_1 \leq \sqrt{1 - F(\rho, \sigma)}. \quad (46)$$

Since the Fuchs-van de Graaf inequalities are not explicitly dependent on the Hilbert-space dimension one can regard the trace distance and fidelity as equivalent measures of quality in many applications. Note however that the square root on the right-hand side can still make a painstaking difference in practice. Aiming at a trace-norm distance of 10^{-3} can in the worst case require to ensure an infidelity of 10^{-6} . This can be a crucial difference when it comes to the feasibility of certification. Importantly, the square-root scaling is unavoidable for pure states.

Lemma 14: (Fuchs-van de Graaf inequality for pure states): The upper bound of the Fuchs-van de Graaf

inequality for pure states $|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi| \in \mathcal{S}(\mathcal{H})$ is tight and the following equality holds for all p ,

$$\| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_p = 2^{1/p} \sqrt{1 - |\langle\psi|\phi\rangle|^2}. \quad (47)$$

Furthermore, show that the equality actually holds for all Schatten p -norms $p \in \{1, 2, \dots, \infty\}$.

Proof. Denote $X := |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|$. We have $\text{Tr}[X] = 0$ and $\text{rank}(X) \in \{0, 2\}$. Hence, X has two eigenvalues $\lambda > 0$ and $-\lambda < 0$. This implies that $\lambda^2 = \|X\|_F^2/2 = 1 - |\langle\psi|\phi\rangle|^2$, as directly follows by writing $\|X\|_F^2$ as a Hilbert-Schmidt inner product. From the eigenvalues one can calculate $\|X\|_p$ as Schatten p -norm, which yields the result. ■

In Lemma 14 we show that the upper bound of Eq. (46) is tight for pure states. Conversely, one might hope for more mixed states to arrive at an improved scaling closer to the lower bound of Eq. (46). We review such a bound in the analogous discussion of distance measures of quantum channels, Theorem 54 in Sec. III A.

In the next section, we present protocols that aim at directly providing an ϵ -certification test for certain states. Sections II H and II J present two protocols that aim at estimating the fidelity: *direct-fidelity estimation* and *shadow-fidelity estimation*.

F. Direct quantum-state certification

In this section we present approaches to certification protocols for quantum states that are direct in that they do not use a protocol designed for another task, such as an estimation protocol, as a subroutine. Our exposition mostly follows the work by Pallister *et al.* [24]. We start with perhaps the most direct attempt building on the insight of Proposition 12. This proposition illustrates the interpretation of the trace distance as the maximal distinguishability by a dichotomic POVM and shows that the optimal POVM in this regard is given by the projection onto the positive part of the state difference. This indicates that the best way to distinguish a pure quantum state from all other states is to measure the POVM that has the state itself as an element.

We now turn this insight into an ϵ -certification test. It can be most easily formulated in terms of the *infidelity* $1 - F$ as the distance measure.

Given a pure target state $\rho = |\psi\rangle\langle\psi|$ with a state vector $|\psi\rangle \in \mathbb{C}^d$, we consider the POVM $\{\Omega, \mathbb{1} - \Omega\}$ given by $\Omega = |\psi\rangle\langle\psi|$. We call the outcome corresponding to Ω “pass” and the one of $\mathbb{1} - \Omega$ “fail”. Then, for any $\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d)$ we have

$$\mathbb{P}[\text{“pass”}] = \text{Tr}[\Omega\tilde{\rho}] = F(\rho, \tilde{\rho}), \quad (48)$$

i.e., the probability of the POVM returning “pass” is the fidelity of the two states. This gives us a simple protocol that measures the POVM on a single state copy and accepts when the result is “pass” and rejects otherwise. This protocol is complete but not sound in the sense of Definition 2 as the probability of an acceptance is fixed to be $1 - F(\rho, \tilde{\rho})$, i.e., the probability of a false acceptance is not constantly bounded away from one. But using more state copies we can boost the probability to detect deviations of the form $F(\rho, \tilde{\rho}) < 1 - \epsilon$ with some targeted confidence $1 - \delta$.

In order to be able to capture a class of large measurement settings we first formulate the protocol for an arbitrary dichotomic POVM measurements.

Protocol 15 (Naive direct quantum-state certification):

Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a pure target state and $\Omega \in \text{Pos}(\mathbb{C}^d)$ with $\|\Omega\|_{\text{op}} \leq 1$. Denote by $\{\Omega, \mathbb{1} - \Omega\}$ the binary POVM given by Ω , call the outcome corresponding to Ω “pass” and the one of $\mathbb{1} - \Omega$ “fail”.

For state preparations $\tilde{\rho}_1, \dots, \tilde{\rho}_{n_{\tilde{\rho}}} \in \mathcal{S}(\mathbb{C}^d)$ the protocol consists of the following steps.

- 1: **for** $i \in [n_{\tilde{\rho}}]$ **do**
- 2: measure $\{\Omega, \mathbb{1} - \Omega\}$ on $\tilde{\rho}_i$
- 3: **if** the outcome is “fail” **then:**
- 4: output “reject” and end protocol
- 5: output “accept”

As stated, this protocol is adaptive in that it can end early in case of a rejection instance. However, one could easily turn into a nonadaptive protocol without changing the number of measurements in the performance guarantee below.

For ρ a pure state and $\Omega = \rho$ the protocol is a certification protocol w.r.t. the infidelity as more precisely summarized by the following proposition.

Proposition 16 (Performance guarantee I): Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a *pure* target state and choose $\epsilon, \delta > 0$. Protocol 15 with $\Omega = \rho$ is an ϵ -certification test w.r.t. the infidelity from $n_{\tilde{\rho}}$ independent samples for

$$n_{\tilde{\rho}} \geq \frac{\ln(1/\delta)}{\epsilon} \quad (49)$$

with confidence at least $1 - \delta$. Moreover, the protocol accepts the target state ρ with probability 1.

Proof. The probability of the measurement outcome “pass” in step $i \in [n_{\tilde{\rho}}]$ is

$$\mathbb{P}[\text{“pass”} | \tilde{\rho}_i] = \text{Tr}[\Omega\tilde{\rho}_i] = \text{Tr}[\rho\tilde{\rho}_i] = F(\rho, \tilde{\rho}_i). \quad (50)$$

Hence, the final probability that the protocol accepts is

$$\mathbb{P}[\text{"accept"}] = \prod_{i=1}^{n_{\tilde{\rho}}} F(\rho, \tilde{\rho}_i). \quad (51)$$

Clearly, if $\tilde{\rho}_i = \rho$ for all $i \in [n_{\tilde{\rho}}]$ then the protocol accepts almost surely. Now let us consider the case that the fidelity is small, i.e.,

$$F(\rho, \tilde{\rho}_i) = \langle \psi | \tilde{\rho}_i | \psi \rangle \leq 1 - \epsilon \quad \forall i \in [n_{\tilde{\rho}}]. \quad (52)$$

Then the probability that the protocol wrongfully accepts is

$$\mathbb{P}[\text{"accept"}] \leq (1 - \epsilon)^{n_{\tilde{\rho}}}. \quad (53)$$

Now we wish this probability (type-II error) be bounded by $\delta > 0$, i.e.,

$$(1 - \epsilon)^{n_{\tilde{\rho}}} \leq \delta. \quad (54)$$

This maximum type-II error is achieved for

$$n_{\tilde{\rho}} \geq \frac{\ln\left(\frac{1}{\delta}\right)}{\ln\left(\frac{1}{1-\epsilon}\right)}. \quad (55)$$

We note that for $\epsilon \in [0, a] \subset [0, 1)$ the following bounds hold:

$$\epsilon \leq \ln\left(\frac{1}{1-\epsilon}\right) \leq \ln\left(\frac{1}{1-a}\right) \frac{\epsilon}{a}, \quad (56)$$

which can be seen by using the fact that $\epsilon \mapsto \ln[1/(1-\epsilon)]$ is smooth, has value 0 at 0, its first derivative is lower bounded by 1, and its second derivative is positive. Hence, for any $n_{\tilde{\rho}} \geq \ln(1/\delta)/\epsilon$ the required bound, Eq. (54), is satisfied. ■

As a remark, the minimum number of samples in Eq. (55) scales as

$$\frac{\ln\left(\frac{1}{\delta}\right)}{\ln\left(\frac{1}{1-\epsilon}\right)} = \frac{\ln(1/\delta)}{\epsilon} + O(1/\epsilon^2), \quad (57)$$

so that Eq. (49) captures the leading scaling of Eq. (55).

Perhaps surprisingly, the sample complexity, Eq. (49), of this direct certification protocol does not depend on the physical system size at all. It has a zero type-I error and one can control the type-II error via the parameter δ . However, for many target states it is not practical to directly implement the required POVM. This motivates the following more complicated strategies. Say, we have access to a set of POVM elements

$$\mathbf{M} \subset \{M \in \text{Pos}(\mathbb{C}^d) : \|M\|_{\text{op}} \leq 1\}. \quad (58)$$

These encode the measurements that are experimentally feasible. As one can only make finitely many measurements, we assume that $|\mathbf{M}| < \infty$. Then for each state we

pick a POVM element $M \in \mathbf{M}$ with some probability and consider the corresponding dichotomic POVMs $\{M, \mathbb{1} - M\}$, where M has output "pass" and $\mathbb{1} - M$ has output "fail". We refer to a set \mathbf{M} of the form, Eq. (58), together with a probability mass $\mu : \mathbf{M} \rightarrow [0, 1]$, $\sum_{M \in \mathbf{M}} \mu(M) = 1$, as a *probabilistic measurement strategy*. Now we modify Protocol 15 by including a probabilistic measurement strategy.

Protocol 17 (Direct state certification): Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a pure target state and (\mathbf{M}, μ) be a probabilistic measurement strategy. For state preparations $\tilde{\rho}_1, \dots, \tilde{\rho}_{n_{\tilde{\rho}}} \in \mathcal{S}(\mathbb{C}^d)$ the protocol consists of the following steps.

- 1: **for** $i \in [n_{\tilde{\rho}}]$ **do**
- 2: Draw M from \mathbf{M} according to μ .
- 3: Measure the POVM $\{M, \mathbb{1} - M\}$ on $\tilde{\rho}_i$.
- 4: **if** the outcome is "fail" **then:**
- 5: output "reject" and end protocol.
- 6: output "accept"

Let us assume that the prepared states are i.i.d. copies of a state $\tilde{\rho}$. Then following Protocol 17 with strategy (\mathbf{M}, μ) the overall probability of measuring "pass" is

$$\mathbb{P}[\text{"pass"}] = \sum_{M \in \mathbf{M}} \mu(M) \text{Tr}[M \tilde{\rho}] = \text{Tr}[\Omega \tilde{\rho}], \quad (59)$$

where

$$\Omega := \sum_{M \in \mathbf{M}} \mu(M) M \quad (60)$$

is the so-called *effective measurement operator*. Below, we see that it plays a similar role as the measurement operator Ω in Protocol 15 when it comes to proving performance guarantees. At the same time, it allows capturing more sophisticated measurement strategies.

However, there is one constraint that allows for a simple analysis of Protocol 17: we require that

$$\text{Tr}[\Omega \rho] = 1, \quad (61)$$

i.e., that there is no false reject of the target state ρ with probability one. In particular, it requires that $\text{Tr}[M \rho] = 1$ for all $M \in \mathbf{M}$. This constraint still allows for optimal measurement strategies.

Proposition 18 ([24, Proposition 8]): Let $\rho = |\psi\rangle\langle\psi|$ be a target state. Let $0 \leq \Omega' \leq \mathbb{1}$ be an effective measurement operator, Eq. (60), with $\text{Tr}[\Omega' \rho] < 1$ so that Protocol 17 is an ϵ -certification test w.r.t. infidelity from $n_{\tilde{\rho}}$ i.i.d. samples. Then there exists an effective measurement operator

$0 \leq \Omega \leq \mathbb{1}$ with $\text{Tr}[\Omega\rho] = 1$ so that Protocol 17 is an ϵ -certification test w.r.t. infidelity from $n_{\tilde{\rho}}$ i.i.d. samples so that $n_{\tilde{\rho}} \leq n_{\tilde{\rho}'}$ holds for sufficiently small ϵ .

The proof of this statement is a consequence of the Chernoff-Stein lemma from information theory, which quantifies the asymptotic distinguishability of two distributions in terms of their relative entropy.

Since the constraint, Eq. (61), implies that there is no *false rejection* the only remaining hypothesis testing error is a *false acceptance*, which is the event where a state $\tilde{\rho}$ with $F(\rho, \tilde{\rho}) < 1 - \epsilon$ is accepted. This event has a worst-case probability over all states $\tilde{\rho}$ in the rejection region that given as

$$\mathbb{P}[\text{"pass"}] = \max_{\substack{\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d): \\ \text{Tr}[\rho\tilde{\rho}] \leq 1-\epsilon}} \text{Tr}[\Omega\tilde{\rho}]. \quad (62)$$

In the following lemma we see that this maximum is determined by the *spectral gap*

$$\nu(\Omega) := \lambda_1(\Omega) - \lambda_2(\Omega), \quad (63)$$

of the effective measurement operator Ω , where $\lambda_1(\Omega) \geq \lambda_2(\Omega) \geq \dots \geq \lambda_d(\Omega)$ are the eigenvalues of Ω in descending order.

Lemma 19 ([24], [25, Supplemental Material, Sec. I]): Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a pure state, $0 \leq \Omega \leq \mathbb{1}$, $\text{Tr}[\rho\Omega] = 1$, and $\epsilon > 0$. Then

$$\max_{\substack{\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d): \\ \text{Tr}[\rho\tilde{\rho}] \leq 1-\epsilon}} \text{Tr}[\Omega\tilde{\rho}] = 1 - \nu(\Omega)\epsilon. \quad (64)$$

Proof. We note that $\text{Tr}[\rho\Omega] = 1$ means that a state vector $|\psi\rangle$ with $\rho = |\psi\rangle\langle\psi|$ is an eigenvalue-1 eigenvector of Ω . Moreover, let us write Ω in spectral decomposition,

$$\Omega = \sum_{j=1}^d \lambda_j P_j, \quad (65)$$

with $1 = \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_d$ and $P_1 = \rho$. For the case $\lambda_2 = 1$ the choice $\tilde{\rho} = P_2$ yields a maximum of 1 in the maximization, Eq. (64). Let us now consider the case $\lambda_2 < 1$. Then for

$$\tilde{\rho} = (1 - \epsilon)\rho + \epsilon P_2 \quad (66)$$

we have

$$\begin{aligned} \text{Tr}[\Omega\tilde{\rho}] &= 1 - \epsilon \text{Tr}[\Omega\rho] + \epsilon \text{Tr}[\Omega P_2] \\ &= 1 - \epsilon + \epsilon \lambda_2 = 1 - (1 - \lambda_2)\epsilon, \end{aligned} \quad (67)$$

i.e., the claimed maximum in Eq. (64) is attained for some feasible σ .

To show that the claimed maximum is actually the maximum we consider some state $\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d)$ with $\text{Tr}[\rho\tilde{\rho}] \leq 1 - \epsilon$. We write $\tilde{\rho}$ as convex combination $\tilde{\rho} = (1 - \epsilon')\rho + \epsilon'\rho^\perp$ and observe that $\epsilon' \geq \epsilon$. Then

$$\begin{aligned} \text{Tr}[\Omega\tilde{\rho}] &= \text{Tr}[\rho\tilde{\rho}] + \sum_{j=2}^d \lambda_j \text{Tr}[P_j\tilde{\rho}] \\ &\leq \text{Tr}[\rho\tilde{\rho}] + \lambda_2 \sum_{j=2}^d \text{Tr}[P_j\tilde{\rho}] \\ &= 1 - \epsilon' + \lambda_2 \epsilon' \text{Tr}\left[\sum_{j=2}^d P_j \rho^\perp\right] \\ &= 1 - \epsilon' + \lambda_2 \epsilon' \text{Tr}[\rho^\perp] \\ &= 1 - \epsilon' + \lambda_2 \epsilon' = 1 - (1 - \lambda_2)\epsilon' \\ &\leq 1 - (1 - \lambda_2)\epsilon. \end{aligned} \quad (68)$$

■

Given a measurement strategy with effective measurement operator Ω this lemma provides a closed formula for the false acceptance probability, Eq. (62). This allows us to state the following guarantee for Protocol 17.

Proposition 20 (Performance guarantee II [24]): Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a pure target state and $\epsilon, \delta > 0$. We consider an effective measurement operator, Eq. (60), satisfying $0 \leq \Omega \leq \mathbb{1}$ and $\text{Tr}[\Omega\rho] = 1$ and having a spectral gap, Eq. (63), bounded as $\nu(\Omega) > 0$. Then the certification test from Protocol 17 is an ϵ -certification test w.r.t. the infidelity from $n_{\tilde{\rho}}$ independent samples for

$$n_{\tilde{\rho}} \geq \frac{\ln(1/\delta)}{\epsilon[1 - \lambda_2(\Omega)]}, \quad (69)$$

with confidence at least $1 - \delta$. Moreover, the protocol accepts the target state ρ with probability 1.

Compared to the sample complexity, Eq. (49), of the naive Protocol 15, the sample complexity, Eq. (69), has an overhead of a factor $1/\nu(\Omega)$,

Proof of Proposition 20. The proof is mostly analogous to the one of Proposition 16.

Thanks to Lemma 19, the probability of wrongfully accepting a state $\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d)$ with $F(\rho, \tilde{\rho}_i) \leq 1 - \epsilon$ is bounded as

$$\mathbb{P}[\text{"pass"}|\tilde{\rho}_i] \leq 1 - \nu(\Omega)\epsilon. \quad (70)$$

Hence, the probability that Protocol 15 accepts is bounded as

$$\mathbb{P}[\text{"accept"}] \leq (1 - \nu(\Omega)\epsilon)^{n_{\tilde{\rho}}}. \quad (71)$$

Imposing $[1 - \nu(\Omega)\epsilon]^{n_{\tilde{\rho}}} \leq \delta$ and solving for $n_{\tilde{\rho}}$ yields

$$n_{\tilde{\rho}} \geq \frac{\ln(1/\delta)}{\ln\left[\frac{1}{1-\nu(\Omega)\epsilon}\right]} \quad (72)$$

and the bound, Eq. (56), finishes the proof. \blacksquare

This proposition tells us that as long as Ω has a constant gap between its largest and second largest eigenvalue the sample complexity of the certification protocol has the same scaling as the one where Ω is the target state itself. Now it depends on the physical situation of what feasible measurement strategies Ω are. Given a set \mathbf{M} of feasible measurements we can single out an optimal strategy as follows.

Definition 21 (Minimax optimization): Let ρ be a pure state and $\epsilon > 0$. Moreover, let us assume that we have access to a compact set of binary measurements given by the operators $\mathbf{M} \subset \{P : 0 \leq P \leq \mathbb{1}, \text{Tr}[P\rho] = 1\}$.

Then the best strategy Ω for the worst-case state preparation $\tilde{\rho}$ is

$$\min_{\Omega \in \text{conv}(\mathbf{M})} \max_{\tilde{\rho}: \text{Tr}[\rho\tilde{\rho}] \leq 1-\epsilon} \text{Tr}[\Omega\tilde{\rho}]. \quad (73)$$

and $\text{conv}(S)$ denotes the *convex hull* of a set S , i.e., the set of all convex combinations of elements in S . This quantity is called *minimax value* and a strategy Ω where the minimum is attained is called *minimax optimal*.

Such minimax optimizations are common in game theory and risk analysis.

If there are no restrictions on the measurements of a pure target state ρ , i.e., $\mathbf{M} = \{P : 0 \leq P \leq \mathbb{1}, \text{Tr}[P\rho] = 1\}$, then $\Omega = \rho$ is minimax optimal.

For a number of settings with physically motivated measurement restrictions, the minimax strategy, or at least one that is close to it, is obtained. For instance, for *stabilizer states*, which are ubiquitous in quantum information. In the following we introduce stabilizer states and, two-outcome Pauli measurements, we derive a minimax optimal certification protocol for them.

1. Stabilizer states

Now we consider the certification of stabilizer target states by using a particularly suitable measurement strategy in the direct certification Protocol 17.

Let us start with a few preliminaries on stabilizer states. An n -qubit *Pauli string* is $\sigma_{s_1} \otimes \cdots \otimes \sigma_{s_n}$, where $s \in \{0, 1, 2, 3\}^n$ and $\{\sigma_i\}$ are the Pauli matrices

$$\begin{aligned} \sigma_x &:= \sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & \sigma_y &:= \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \\ \sigma_z &:= \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & \sigma_0 &:= \mathbb{1}_{2 \times 2}. \end{aligned} \quad (74)$$

Then the *Pauli group* $\mathcal{P}_n \subset U(2^n)$ is the group generated by all n -qubit Pauli strings and $i\mathbb{1}$. An n -qubit state $|\psi\rangle$ is a *stabilizer state* if there is an Abelian subgroup $\mathcal{S} \subset \mathcal{P}_n$, called *stabilizer (subgroup)*, that stabilizes $|\psi\rangle$ and only $|\psi\rangle$, i.e., $|\psi\rangle$ is the unique joint eigenvalue-1 eigenstate of all elements in that subgroup. Such subgroups are generated by n elements and contain $|\mathcal{S}| = 2^n$ elements in total. Note that they cannot contain the element -1 .

An example of such a subgroup is the one of all Pauli strings made of $\mathbb{1}$'s and σ_z 's.

It is not difficult to show that a general n -qubit stabilizer state ρ with stabilizer \mathcal{S} is explicitly given as

$$\rho = \frac{1}{2^n} \sum_{S \in \mathcal{S}} S. \quad (75)$$

The measurement strategy for our direct certification of stabilizer states essentially consists in measuring stabilizer observables that are drawn uniformly at random from the stabilizer group of the target state. We accept exactly when the measurement outcome corresponds to the stabilized eigenspaces of eigenvalue $+1$. This strategy is minimax optimal (Definition 21) among all strategies based on measuring Pauli observables, i.e., two-outcome Pauli measurements.

Theorem 22: (Minimax optimal two-outcome Pauli measurements for STABs [24]): Let $|\psi\rangle$ be an n -qubit stabilizer state with stabilizer group $\mathcal{S} \subset \mathcal{P}_n$ with elements $\mathcal{S} = \{\mathbb{1} = S_0, S_1, \dots, S_{2^n-1}\}$. For $i \in [2^n - 1]$ denote by $P_i := \frac{1}{2}(\mathbb{1} + S_i)$ the projector onto the positive eigenspace of S_i .

Then the minimax optimal measurement strategy for having Pauli observables \mathcal{P}_n as accessible measurements (see Definition 21) is given by measuring S_i with probability $1/(2^n - 1)$. The resulting effective measurement operator $\Omega = 1/(2^n - 1) \sum_{i=1}^{2^n-1} P_i$ satisfies $\Omega|\psi\rangle = |\psi\rangle$ and has the second largest eigenvalue

$$\lambda_2(\Omega) = \frac{2^{n-1} - 1}{2^n - 1}. \quad (76)$$

Proof. By Lemma 19, the minimax optimum is

$$\begin{aligned} \min_{\Omega \in \mathcal{X}} \max_{\tilde{\rho}: \text{Tr}[\rho\tilde{\rho}] \leq 1-\epsilon} \text{Tr}[\Omega\tilde{\rho}] &= \min_{\Omega \in \mathcal{X}} [1 - \nu(\Omega)\epsilon] \\ &= 1 - \epsilon \max_{\Omega \in \mathcal{X}} \nu(\Omega), \end{aligned} \quad (77)$$

where

$$\mathcal{X} := \{\Omega \in \text{conv}(\mathcal{P}_n) : \Omega|\psi\rangle = |\psi\rangle\} = \text{conv}(\mathcal{S}). \quad (78)$$

We argue that the minimization over $\text{conv}(\mathcal{S})$ can be replaced by a minimization over $\text{conv}(\mathcal{S}')$ with $\mathcal{S}' := \mathcal{S} \setminus \{\mathbb{1}\}$. To see this, observe that if $\Omega = (1 - \alpha)\Omega' + \alpha\mathbb{1}$

for $\alpha \in [0, 1]$ then $\nu(\Omega) \leq \nu(\Omega')$. Then minimax optimal measurement strategies are of the form

$$\Omega = \sum_{i=1}^{2^n-1} \mu_j P_i, \quad (79)$$

for a probability vector μ . We note that

$$\text{Tr}[\Omega] = 2^{n-1} \quad (80)$$

since $\text{Tr}[P_i] = 2^{n-1}$.

Next, since $|\psi\rangle$ is an eigenvalue-1 eigenvector of Ω , we have

$$\Omega = \mathbb{1} \oplus \tilde{\Omega} \quad (81)$$

and, hence

$$\lambda_2(\Omega) = \|\tilde{\Omega}\|_{\text{op}}. \quad (82)$$

Moreover, $\text{Tr}[\tilde{\Omega}] = 2^{n-1} - 1$. The operator $\tilde{\Omega}$ with the minimal norm $\|\tilde{\Omega}\|_{\text{op}}$ under this constraint is of the form $\tilde{\Omega} = a\mathbb{1}$ for $a > 0$. Taking the trace of that equality, solving for a and denoting the orthogonal projector of $|\psi\rangle\langle\psi|$ by $|\psi\rangle\langle\psi|^\perp := \mathbb{1} - |\psi\rangle\langle\psi|$ yields

$$\Omega = |\psi\rangle\langle\psi| + \frac{2^{n-1} - 1}{2^n - 1} |\psi\rangle\langle\psi|^\perp, \quad (83)$$

with

$$\lambda_2(\Omega) = \frac{2^{n-1} - 1}{2^n - 1}. \quad (84)$$

In order to finish the proof we show that $\Omega \in \text{conv}(\mathcal{S})$, i.e., that this choice of Ω is indeed compatible with Eq. (79).

We write the stabilizer state $|\psi\rangle\langle\psi|$ as combination of the stabilizers [see Eq. (75)] and use that $S_j = 2P_j - \mathbb{1}$,

$$\begin{aligned} |\psi\rangle\langle\psi| &= \frac{1}{2^n} \left(\mathbb{1} + \sum_{j=1}^{2^n-1} S_j \right) \\ &= \frac{1}{2^n} \left[\mathbb{1} + 2 \sum_{j=1}^{2^n-1} P_j - (2^n - 1)\mathbb{1} \right] \\ &= \left(\frac{1}{2^{n-1}} - 1 \right) \mathbb{1} + \frac{1}{2^{n-1}} \sum_{j=1}^{2^n-1} P_j. \end{aligned} \quad (85)$$

With $\mathbb{1} = |\psi\rangle\langle\psi| + |\psi\rangle\langle\psi|^\perp$ this implies

$$\sum_{j=1}^{2^n-1} P_j = (2^n - 1)|\psi\rangle\langle\psi| + (2^{n-1} - 1)|\psi\rangle\langle\psi|^\perp \quad (86)$$

and, hence

$$\frac{1}{2^n - 1} \sum_{j=1}^{2^n-1} P_j = |\psi\rangle\langle\psi| + \frac{2^{n-1} - 1}{2^n - 1} |\psi\rangle\langle\psi|^\perp, \quad (87)$$

which is the Ω from Eq. (83) and also the measurement strategy from the theorem statement. \blacksquare

Corollary 23 (Sampling complexity [24]): Let us call the outcome corresponding to P_i “pass” and the one corresponding to $1 - P_i$ “fail”. Then Protocol 17 is an ϵ -certification test of ρ w.r.t. infidelity from $n_{\tilde{\rho}}$ independent samples for

$$n_{\tilde{\rho}} \geq 2 \frac{\ln(1/\delta)}{\epsilon}, \quad (88)$$

with confidence $1 - \delta$. Moreover, ρ is accepted with probability 1.

Proof. According to Proposition 20 a number of measurements

$$n_{\tilde{\rho}} \geq \frac{\ln(1/\delta)}{\epsilon \nu(\Omega)} \quad (89)$$

is sufficient, where

$$\begin{aligned} \nu(\Omega) &= 1 - \lambda_2(\Omega) \\ &= 1 - \frac{2^{n-1} - 1}{2^n - 1} \\ &= \frac{2^{n-1}}{2^n - 1}. \end{aligned} \quad (90)$$

This results in

$$n_{\tilde{\rho}} \geq \frac{2^n - 1}{2^{n-1}} \frac{\ln(1/\delta)}{\epsilon}. \quad (91)$$

\blacksquare

So, restricting from all measurements to Pauli measurements results in at most a constant overhead of 2, cmp. Proposition 16. We note that only very few of the $2^n - 1$ nontrivial stabilizers of ρ are actually measured. More precisely, the measurements are the ones of randomly subsampled stabilizer observables.

2. Extension towards fidelity estimation

Direct certification provides minimum information to solve the certification task by just accepting or rejecting. Often it is also desirable to actually know explicitly what the distance or fidelity of a quantum-state implementation $\tilde{\rho}$ to its target ρ is.

The direct quantum-state certification protocol, Eq. (17), with effective measurement operator Ω [see Eq. (60)] can

be turned into an estimation protocol for the fidelity $F(\tilde{\rho}, \rho)$ if Ω is *homogeneous*, i.e., of the form

$$\Omega = |\psi\rangle\langle\psi| + \tau|\psi\rangle\langle\psi|^\perp \quad (92)$$

for some $\tau > 0$ [14,26]; for instance, for stabilizer states, Eq. (83) we have $\tau = [(2^{n-1} - 1)/(2^n - 1)]$. In this case, we have

$$\text{Tr}[\tilde{\rho}\Omega] = F(\tilde{\rho}, \rho) + \tau\{\text{Tr}[\tilde{\rho}] - F(\tilde{\rho}, \rho)\} \quad (93)$$

and, hence,

$$F(\tilde{\rho}, \rho) = \frac{\text{Tr}[\tilde{\rho}\Omega] - \tau}{1 - \tau} = \frac{\text{Tr}[\tilde{\rho}\Omega] - \lambda_2(\Omega)}{\nu(\Omega)}. \quad (94)$$

Therefore, an estimate on the expectation value of Ω yields an estimate of the fidelity $F(\tilde{\rho}, \rho)$.

We note that the number of measurements required for estimating the expectation value up to an additive error ε scales as $1/\varepsilon^2$. We also remember that in the case where we can measure Ω as observable the estimation task can be solved with a number of measurements $m \geq (1/2\varepsilon^2) \ln(2/\delta)$ with confidence $1 - \delta$, see Proposition 10. However, in Protocol 17 we only assume access to measurements $M \in \mathbb{M}$ that on some average give the expectation value of Ω . In general, the number of measurements $|\mathbb{M}|$ can be exponentially large, as is the case for stabilizer states, cp. Theorem 22. Here, one could use ideas of Monte Carlo estimation and importance sampling in order to perform this estimation efficiently; a method that we introduce in Sec. II G. Subsequently, we discuss direct-fidelity estimation, which relies on this idea.

Further reading

The direct certification of maximally entangled states was studied by Hayashi *et al.* [27,28]. Building on these earlier works and the discussed framework of Pallister *et al.* [24], direct certification protocols were then developed for other classes of quantum states featuring a (close to) optimal sampling complexity. They include the following settings:

- (a) Stabilizer states and two-qubit states with single-qubit measurements [24].
- (b) Bipartite states [26,29], qubit case in an LOCC setting [30].
- (c) Hypergraph states [11] with improvements in efficiency by Zhu and Hayashi [25] and a generalization to weighted graph states [31].
- (d) Dicke states [32,33].

- (e) A general adversarial scenario without the assumptions of the state preparations being identical and independent [13,14].

Protocols for the efficient verification of graph states, which are certain stabilizer states, were developed in the context of measurement-only blind quantum computation [34] and interactive proof systems [35,36].

Efficient certification protocols for ground states of locally interacting Hamiltonians were developed by Cramer *et al.* [37] and extended by Hangleiter *et al.* [38] to ground states enabling universal quantum computation. In this line of research, fidelity witnesses [38–40] can be used to measure and estimate on a fidelity lower bounds. Also in the context of interactive proof systems efficient ground-state certification schemes have been developed [36,41].

Kalev *et al.* [42] have extended arguments from direct-fidelity estimation [43] (see Sec. II H) and ground-state certification [38] to the certification of stabilizer states. They also use Bernstein’s inequality to give a quadratically improved ϵ -scaling for large ϵ .

The work [37] solves the certification problem by efficiently reconstructing the state assuming it to be of matrix product form. Similar ideas based on ansatz state tomography also work for permutationally invariant states [44–46].

Takeuchi and Morimae [11] provide efficient results on the certification of ground states of locally interacting Hamiltonians, and hypergraph states, where the i.i.d. assumptions on the state preparations is removed using a quantum de Finetti theorem [12]. Hypergraph states include quantum states that are generated by so-called IQP circuits designed for demonstrating quantum supremacy [47].

Global von Neumann measurements on multiple i.i.d. copies of the prepared quantum state have been considered [48] (even with mixed target states), which leads to a sample complexity scaling as $n_{\tilde{\rho}} \in O(d/\epsilon)$ a version of ϵ -certification of quantum states in $\mathcal{S}(\mathbb{C}^d)$.

For a very helpful survey on *quantum property testing* we refer to Ref. [49], where several methods and notions of certification are reviewed.

G. Importance sampling

In the next section, we study direct-fidelity estimation, where the fidelity between a target state and a state preparation is estimated from measurements that are drawn randomly from a certain distribution depending on the target state. The idea is to perform the measurements more often that are particularly relevant to the fidelity estimation.

This idea is formalized by a Monte Carlo integration technique called *importance sampling*. Monte Carlo integration aims at computing an integral F that is written as

an expected value of some function f over a probability distribution with density function p :

$$F := \mathbb{E}_{X \sim p}[f(X)] = \int f(x)p(x)dx. \quad (95)$$

The general idea is to draw i.i.d. samples $X^{(1)}, \dots, X^{(m)} \sim p$ and take the empirical average

$$\hat{F} := \frac{1}{m} \sum_{i=1}^m f(X^{(i)}) \quad (96)$$

as estimator for F . It is not difficult to see that \hat{F} is unbiased. If $\text{Var}[f(X)] < \infty$ then \hat{F} can be proven to be *consistent*, i.e., \hat{F} converges to F for $m \rightarrow \infty$ in an appropriate sense. Moreover,

$$\text{Var}[\hat{F}] = \frac{\text{Var}[f(X)]}{m}. \quad (97)$$

Thereby the empirical variance also gives an estimate of the estimation error. The estimation error can be controlled by increasing the number of samples m .

Now, the integration, Eq. (96), relies on the ability to sample from p . A popular way to make such sampling efficient is *importance sampling*. The main idea of importance sampling is to rewrite the integrand fp in Eq. (95) as

$$fp = \frac{fp}{q}q \quad (98)$$

for some probability distribution with density function q . Then we can apply the Monte Carlo sampling idea (96) with respect to q and draw $X^{(1)}, \dots, X^{(m)} \sim q$ i.i.d. to obtain the estimator

$$\hat{F}_q := \frac{1}{m} \sum_{i=1}^m f[X^{(i)}] \frac{p[X^{(i)}]}{q[X^{(i)}]}. \quad (99)$$

It holds that $\mathbb{E}_q[\hat{F}_q] = F$ and

$$\text{Var}_q[\hat{F}_q] = \frac{1}{m} \text{Var}_q[fp/q] = \frac{1}{m} \left[\int \frac{f^2 p^2}{q} - F^2 \right]. \quad (100)$$

One can show that the minimal variance is achieved by choosing q as

$$q^* := \frac{p|f|}{Z} \quad (101)$$

with a normalization factor Z such that q^* is a probability density. Note that for $f \geq 0$ we have $\mathbb{E}_{q^*}[(fp/q^*)^2] = \mathbb{E}_p[f^2] = \mathbb{E}_{q^*}[fp/q^*]^2$ and, thus, $\text{Var}_{q^*}[\hat{F}_{q^*}] = 0$. So, if f does not change its sign then a single sample from q^*

is sufficient for the exact estimation. This might seem miraculous at first sight. But it is important to notice that in order to determine the optimal q^* one needs to know the value of normalization Z and calculating Z is equivalent to solving the integration problem. However, finding nonoptimal but good choices for q can already speed up the integration, as we see in the case of direct-fidelity estimation.

H. Direct-fidelity estimation

We assume to be given access to state preparations $\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d)$ of some target state $\rho \in \mathcal{S}(\mathbb{C}^d)$. *Direct-fidelity estimation (DFE)* [43,50] is a protocol to estimate the fidelity $\text{Tr}[\tilde{\rho}\rho]$ for the case where the ρ is a pure state, i.e., of the form $\rho = |\psi\rangle\langle\psi|$. In order to do so, the target states is expanded into products of Pauli matrices, Eq. (74), of the form $\sigma_{s_1} \otimes \dots \otimes \sigma_{s_n}$ with $s_i \in \{0, \dots, 4\}$ and $d = 2^n$ being the Hilbert space dimension. For sake of readability we denote these Pauli products by W_1, \dots, W_{d^2} in some order and note that they are an orthogonal basis for the space of Hermitian operators $\text{Herm}(\mathbb{C}^d)$ with respect to the Hilbert-Schmidt inner product, Eq. (1),

$$\frac{1}{d} \text{Tr}[W_k W_{k'}] = \delta_{k,k'} \quad (102)$$

for all $k, k' \in [d^2]$.

Given any operator $\sigma \in \text{Herm}(\mathbb{C}^d)$ we define its *characteristic function* (or *quasiprobability distribution*) $W_\sigma : [d^2] \rightarrow \mathbb{R}$ by

$$\chi_\sigma(k) := \text{Tr} \left[\sigma \frac{W_k}{\sqrt{d}} \right]. \quad (103)$$

Thanks to the orthogonality relation, Eq. (102), we have

$$\sigma = \sum_{k=1}^{d^2} \chi_\sigma(k) \frac{W_k}{\sqrt{d}} \quad (104)$$

and hence

$$\text{Tr}[\rho\sigma] = \sum_{k=1}^{d^2} \chi_{\tilde{\rho}}(k) \chi_\sigma(k) \quad (105)$$

for any $\rho, \sigma \in \text{Herm}(\mathbb{C}^d)$.

Now, we use *importance sampling* (Sec. II G) to estimate the sum, Eq. (105), for the case where the target state $\rho \in \mathcal{S}(\mathbb{C}^d)$ is a pure state. For this purpose we rewrite the overlap, Eq. (105), as

$$\text{Tr}[\rho\tilde{\rho}] = \sum_{k=1}^{d^2} \frac{\chi_{\tilde{\rho}}(k)}{\chi_\rho(k)} \chi_\rho(k)^2 \quad (106)$$

and define

$$q_k := \chi_\rho(k)^2. \quad (107)$$

We choose q as the probability mass function of the importance sampling distribution on the sampling space $[d^2]$. The purity of ρ can be written as

$$\text{Tr}[\rho^2] = \sum_{k=1}^{d^2} \left| \left\langle \frac{W_k}{\sqrt{d}}, \rho \right\rangle \right|^2 = \sum_{k=1}^{d^2} \chi_\rho(k)^2 \quad (108)$$

and equals 1 for ρ pure. Thus, q is indeed a normalized probability vector.

We define random variable

$$X_k := \frac{\chi_{\tilde{\rho}}(k)}{\chi_\rho(k)} \quad (109)$$

for $k \sim q$ and find that X_k is an unbiased estimator of the fidelity:

$$\mathbb{E}_{k \sim q}[X_k] = \sum_{k=1}^{d^2} \frac{\chi_{\tilde{\rho}}(k)}{\chi_\rho(k)} q_k = \sum_{k=1}^{d^2} \chi_\rho(k) \chi_{\tilde{\rho}}(k) = \text{Tr}[\rho \tilde{\rho}], \quad (110)$$

where the last identity is again Eq. (105).

In order to estimate the random variable X_k , we need to know the value of the characteristic function $\chi_{\tilde{\rho}}(k)$. By Eq. (103), $\chi_{\tilde{\rho}}(k)$ can be estimated as the expectation value from repeated measurements of the observable W_k in the prepared state $\tilde{\rho}$. Thus, we end up with an estimation procedure of $\text{Tr}[\rho \tilde{\rho}]$ that involves two sources of randomness and correspondingly proceeds in two steps. (i) We classically sample k from $[d^2]$ according to the importance sampling distribution, Eq. (107), defined by the target state ρ . (ii) For the randomly drawn k , we estimate X_k from repeated probabilistic measurements of W_k . Combining the estimates of the X_k we arrive at an estimate for $\text{Tr}[\rho \tilde{\rho}]$ via Eq. (110).

The following protocol summarizes these steps.

Protocol 24 (DFE [43]): Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a pure target state and $\{W_k\}$ a set of observables $\{W_k\}$. Let $\epsilon > 0$ and $\delta > 0$ be the parameters for the desired estimation accuracy and maximum failure probability.

The protocol consists of the following steps in total requiring $n_{\tilde{\rho}}$ state preparations.

(i) Draw i.i.d. samples $k_1, \dots, k_\ell \sim q$ from the importance sampling distribution, Eq. (107), where $\ell := \lceil 1/\epsilon^2 \delta \rceil$ [or as Eq. (131) for well-conditioned states].

(ii) Measure each observable W_{k_i} a number of m_i times for $i \in [\ell]$ with m_i chosen as

$$m_i := \left\lceil \frac{2}{d \chi_\rho(k_i)^2 \ell \epsilon^2} \ln(2/\delta) \right\rceil \quad (111)$$

(or as $m_i = 1$ for well-conditioned states).

(iii) For each $i \in [\ell]$ calculate empirical estimate of the expectation value $\langle W_{k_i} \rangle_{\tilde{\rho}}$ from the measurement outcomes. From these estimates calculate the estimator \hat{X}_{k_i} for $X_{k_i} := \chi_{\tilde{\rho}}(k_i)/\chi_\rho(k_i) = \langle W_{k_i} \rangle_{\tilde{\rho}} / \sqrt{d} \chi_\rho(k_i)$.

(iv) Calculate $\hat{Y} := \frac{1}{\ell} \sum_{i=1}^{\ell} \hat{X}_{k_i}$.

(v) Output \hat{Y} as a fidelity estimator.

To derive a guarantee for DFE we have to control the error made in the two estimation steps. To this end, we consider the steps in reversed order: we consider $Y := (1/\ell) \sum_{i=1}^{\ell} X_{k_i}$ with ℓ i.i.d. samples $k_i \sim q$ assuming perfect estimates X_{k_i} for the moment. The accuracy of Y as an estimator of $\text{Tr}[\rho \tilde{\rho}]$ can be controlled by increasing ℓ . Subsequently, we have to analyze the accuracy of the estimator \hat{Y} of Y that uses the finitely many measurement outcomes. Altogether we arrive at the following guarantee.

Theorem 25 (Guarantee for DFE [43]): Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a pure target state. The number of expected state preparations in Protocol 24 is

$$\mathbb{E}[n_{\tilde{\rho}}] = \mathbb{E} \sum_{i=1}^{\ell} m_i \leq 1 + \frac{1}{\epsilon^2 \delta} + \frac{2d}{\epsilon^2} \ln(2/\delta). \quad (112)$$

If the state preparations are i.i.d. given by $\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d)$ then the fidelity estimate \hat{Y} is an 2ϵ -accurate unbiased estimator of $F(\rho, \tilde{\rho})$ with confidence $1 - 2\delta$.

Note that the sample complexity scales linearly in the Hilbert space dimension. In contrast, the number of Pauli measurements required for state tomography scales as $\tilde{\Omega}[d^2 \text{rank}(\tilde{\rho})^2]$ [15].

Proof of Theorem 25. We start with bounding the estimation error arising by taking the empirical average in step (iv) of Protocol 24. We note that X_k defined in Eq. (109) is an unbounded random variable in general, as $\chi_\rho(k)$ can be arbitrarily small. Hence, we use Chebyshev's inequality, Eq. (22), to derive a tail bound for Y . Using the definitions, Eqs. (107) and (109), of q and X and that X is the unbiased estimator, Eq. (110), the variance of X becomes

$$\begin{aligned} \text{Var}_{k \sim q}[X_k] &= \mathbb{E}_{k \sim q}[X_k^2] - \text{Tr}[\rho \sigma]^2 \\ &= \sum_{k=1}^{d^2} \frac{\chi_{\tilde{\rho}}(k)^2}{\chi_\rho(k)^2} \chi_\rho(k)^2 - \text{Tr}[\rho \sigma]^2 \\ &= \chi_{\tilde{\rho}}(k)^2 - \text{Tr}[\rho \sigma]^2 \\ &= \text{Tr}[\tilde{\rho}^2] - \text{Tr}[\rho \tilde{\rho}]^2. \end{aligned} \quad (113)$$

Hence,

$$\text{Var}_{k \sim q}[X_k] \leq \text{Tr}[\tilde{\rho}^2] \leq 1. \quad (114)$$

Using the basic insight of Monte Carlo estimation, Eq. (97), we obtain

$$\text{Var}_q[Y] = \mathbb{E}_q\{(Y - \text{Tr}[\rho\tilde{\rho}])^2\} \leq 1/\ell. \quad (115)$$

As Y is an unbiased estimator of $\text{Tr}[\rho\tilde{\rho}]$, i.e., $\mathbb{E}_q(Y - \text{Tr}[\rho\tilde{\rho}]) = 0$, we can directly apply Chebyshev's inequality, Eq. (22), to arrive at

$$\mathbb{P}(|Y - \text{Tr}[\rho\tilde{\rho}]| \geq \epsilon) \leq \frac{1}{\epsilon^2 \ell} \quad (116)$$

for any $\epsilon > 0$. Hence, for any $\delta > 0$ and

$$\ell \geq \frac{1}{\epsilon^2 \delta} \quad (117)$$

the failure probability is bounded by δ ,

$$\mathbb{P}(|Y - \text{Tr}[\rho\tilde{\rho}]| \geq \epsilon) \leq \delta. \quad (118)$$

Now we bound the statistical error that arises from the estimation of X_{k_i} from the measurement setup $i \in [\ell]$ in step (iii) of Protocol 24. For this purpose we write for each k the eigendecomposition of W_k as

$$W_k = \sum_{\alpha} a_{k,\alpha} P_{k,\alpha}, \quad (119)$$

with $\{P_{k,\alpha}\}$ being the projector onto the eigenspaces and $\{a_{k,\alpha}\} \subset \{-1, 1\}$ the eigenvalues of the Pauli string W_k . We note that the expected measurement outcome is

$$\mathbb{E}[a_{k,\alpha}] = \text{Tr}[W_k \tilde{\rho}] = \sqrt{d} \chi_{\tilde{\rho}}(k). \quad (120)$$

We denote by a_{k_j, α_j} the measurement outcome for measurement $j \in [m_i]$ and consider the following corresponding empirical estimate of X_{k_i} [see Eq. (109)]

$$\hat{X}_{k_i} := \frac{1}{m_i \sqrt{d} \chi_{\rho}(k_i)} \sum_{j=1}^{m_i} a_{k_j, \alpha_j}. \quad (121)$$

Then we consider the sum

$$\begin{aligned} \ell \hat{Y} &= \sum_{i=1}^{\ell} \hat{X}_{k_i} \\ &= \sum_{i=1}^{\ell} \sum_{j=1}^{m_i} \frac{1}{m_i \sqrt{d} \chi_{\rho}(k_i)} a_{k_j, \alpha_j}. \end{aligned} \quad (122)$$

As $\mathbb{E}[\ell \hat{Y}] = \ell Y$, using Hoeffding's inequality, Eq. (24), on the double sum with $t = \epsilon \ell$ and bounds

$$b_i = -a_i = \frac{1}{m_i \sqrt{d} \chi_{\rho}(k_i)}, \quad (123)$$

we find that [without loss of generality we assume that there are no i with $\chi_{\rho}(k_i) = 0$]

$$\begin{aligned} \mathbb{P}[|\hat{Y} - Y| \geq \epsilon] &= \mathbb{P}[|\ell \hat{Y} - \ell Y| \geq \ell \epsilon] \\ &\leq 2 \exp \left[\frac{-2\epsilon^2 \ell^2}{\sum_{i=1}^{\ell} \sum_{j=1}^{m_i} \frac{2^2}{m_i^2 d \chi_{\rho}(k_i)^2}} \right] \\ &= 2 \exp \left[\frac{-\epsilon^2 \ell^2}{\sum_{i=1}^{\ell} \frac{2}{m_i d \chi_{\rho}(k_i)^2}} \right]. \end{aligned} \quad (124)$$

We wish that the tail bound

$$\mathbb{P}[|\hat{Y} - Y| \geq \epsilon] \leq \delta \quad (125)$$

holds. Therefore, we impose the right-hand side of Eq. (124) to be bounded by δ , which is equivalent to

$$\ln(2/\delta) \leq \frac{\epsilon^2 \ell^2}{\sum_{i=1}^{\ell} \frac{2}{m_i d \chi_{\rho}(k_i)^2}}. \quad (126)$$

The choice of m_i as in Eq. (111) guarantees that this bound is always satisfied and, thus, Eq. (125) holds. Then combination of the tails bounds, Eqs. (118) and (125), with the union bound, Eq. (29), proves the confidence statement,

$$\mathbb{P}[|\hat{Y} - F(\rho, \tilde{\rho})| \leq 2\epsilon] \geq 1 - 2\delta. \quad (127)$$

In order to calculate the final sample complexity, Eq. (112), note that m_i is a random variable itself, since k_i and hence $\chi_{\rho}(k_i)$ is randomly chosen. By the definition of the sampling, Eq. (107), for fixed i we have

$$\begin{aligned} \mathbb{E}[m_i] &= \sum_{k_i=1}^{d^2} m_i q_{k_i} \\ &\leq 1 + \frac{2d}{\ell \epsilon^2} \ln(2/\delta), \end{aligned} \quad (128)$$

where the $+1$ comes from the ceiling in Eq. (111). Using the bound, Eq. (117), on ℓ , the expected total number of measurements is

$$\mathbb{E} \sum_{i=1}^{\ell} m_i \leq 1 + \frac{1}{\epsilon^2 \delta} + \frac{2d}{\epsilon^2} \ln(2/\delta). \quad (129)$$

■

We remark that DFE estimation can be extended to sets of observables that are arbitrary orthonormal bases of $\text{Herm}(\mathbb{C}^d)$. However, in this case the operator norm used to bound the eigenvalues $a_{k,\alpha}$ and hence the sampling complexity can be larger. One can generalize DFE further to frames that include over-complete bases, see Ref. [51].

The main contribution to the number of measurements in the derivation of the sample complexity above can be traced back to the application of Chebyshev's inequality in Eq. (116). This step can, however, be improved for the following class of states.

Definition 26 (Well-conditioned states): We call an operator $\rho \in \text{Herm}(\mathbb{C}^d)$ *well-conditioned with parameter* $\alpha > 0$ if for each $k \in [d^2]$ either $|\text{Tr}[W_k \rho]| \geq \alpha$ or $\text{Tr}[W_k \rho] = 0$.

A prominent example for well-conditioned states are stabilizer states, Eq. (75). It is easy to show that every stabilizer state ρ on n qubits with stabilizer \mathcal{S} , Eq. (75), is well conditioned with parameter $\alpha = 1$:

$$\text{Tr}[W_k \rho] = \frac{1}{d} \sum_{S \in \mathcal{S}} \text{Tr}[W_k S] \in \{-1, 0, 1\}, \quad (130)$$

where the sum evaluates to 1 if $W_k \in \mathcal{S}$, to -1 if $-W_k \in \mathcal{S}$ and to 0 otherwise.

For such well-conditioned states the sample complexity can be improved as follows.

Theorem 27 (DFE, well-conditioned states [43]): Let $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a pure target state that is well conditioned with parameter $\alpha > 0$. Consider the estimator \hat{Y} from Protocol 24 modified by setting $m_i = 1$ for all $i \in [\ell]$ in step (ii) of Protocol 24 and

$$\ell := \left\lceil \frac{2}{\alpha^2 \epsilon^2} \ln(2/\delta) \right\rceil \quad (131)$$

in step (i) of Protocol 24. If the state preparations are i.i.d. given by $\tilde{\rho} \in \mathcal{S}(\mathbb{C}^d)$ then the fidelity estimate \hat{Y} is an ϵ -accurate unbiased estimator of $F(\rho, \tilde{\rho})$ with confidence $1 - \delta$.

Proof. With probability 1 we have $\sqrt{d} \chi_\rho(k_i) \geq \alpha$ for all $i \in [\ell]$. Moreover, $|\sqrt{d} \chi_{\tilde{\rho}}(k_i)| \leq 1$. The estimator from step (iii) of Protocol 24 is hence bounded as

$$|X_{k_i}| \leq \frac{1}{\alpha} \quad (132)$$

with probability 1. The estimator \hat{Y} is, thus, bounded as $|\hat{Y}| \leq 1/\alpha$ almost surely. Hoeffding's inequality (24) with

$t = \epsilon \ell$ yields

$$\mathbb{P}\left(\left|\hat{Y} - \text{Tr}[\rho \tilde{\rho}]\right| \geq \epsilon\right) \leq 2 \exp\left(-\frac{\ell \alpha^2 \epsilon^2}{2}\right). \quad (133)$$

Imposing

$$2 \exp\left(-\frac{\ell \alpha^2 \epsilon^2}{2}\right) \leq \delta \quad (134)$$

and solving for ℓ we find that

$$\mathbb{P}[|\hat{Y} - F(\rho, \tilde{\rho})| \leq \epsilon] \geq 1 - \delta. \quad (135)$$

■

Theorem 27 tells us that for well-conditioned states DFE has a sampling complexity independent of the system size. Reference [43] investigates the idea of removing ‘‘bad events,’’ which are those that violate the well-conditioning condition. Moreover, a two-step estimation procedure as in Theorem 25 is considered also for well-conditioned states.

Finally, we look at how to turn DFE into a certification protocol with respect to the trace distance.

We summarize the result in the following proposition.

Proposition 28: (Certification with respect to the trace distance via DFE): Fix parameters $\tilde{\epsilon}, \epsilon, \delta > 0$ with $\tilde{\epsilon} \leq \frac{1}{2}\epsilon^2$. Let \hat{Y} be the direct-fidelity estimator of the fidelity $F(\rho, \sigma)$ so that $|\hat{Y} - F(\rho, \sigma)| \leq \tilde{\epsilon}$ with confidence $1 - \delta$. We consider the protocol that *accepts* if $\hat{Y} \geq 1 - \tilde{\epsilon}$ and *rejects* otherwise. We choose the trace distance $\text{dist}_{\text{Tr}}(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1$ as the distance measure.

(i) This protocol is an ϵ -certification test w.r.t. the trace distance in the sense of Proposition 4, i.e., the completeness and soundness conditions are satisfied with confidence $1 - \delta$.

(ii) The resulting sampling complexity of DFE for well-conditioned states scales as $1/\epsilon^4$.

(iii) Let $\epsilon' < \epsilon$. This protocol can be turned into a *robust* (ϵ, ϵ') -certification test, i.e., into an ϵ -certification test that is guaranteed to accept all states within an ϵ' -trace norm ball around ρ with confidence $1 - \delta$.

Proof. The proof follows from Definition 2 by direct calculations. We leave filling in the details as an exercise. ■

I. Random states and unitaries

Random ensembles of quantum states and unitary matrices find ubiquitous applications in quantum-information processing and, in particular, in certification and estimation protocols. Roughly speaking, random unitary operations together with a fixed quantum measurement allow information about the entire state space to be quickly gained.

Arguably the simplest probability distribution on the unitary group $U(d)$ is given by the *Haar measure* $\mu_{U(d)}$. In general, for a compact Lie group the Haar measure is the unique left and right invariant probability measure, which generalizes the notion of a uniform measure. In applications one is often interested in random variables that are polynomials in matrix elements of a Haar random unitary U and its complex-conjugate U^\dagger . In this case, also all moments of the random variable are the expected value of such polynomials. In this section we introduce the mathematical theory required to explicitly calculate such moments. To this end, we observe that any polynomial $p_r(U, U^\dagger)$ of degree k can be written as the contraction with two matrices $A, B \in \mathbb{C}^{dk \times dk}$

$$p_k(U, U^\dagger) = \text{Tr}[BU^{\otimes k}A(U^\dagger)^{\otimes k}]. \quad (136)$$

This motivates the definition of the *kth moment operator* of a probability measure μ on $U(d)$ as $\mathcal{M}_\mu^{(k)} : \mathbb{C}^{dk \times dk} \rightarrow \mathbb{C}^{dk \times dk}$,

$$\begin{aligned} \mathcal{M}_\mu^{(k)}(A) &= \mathbb{E}_{U \sim \mu} [U^{\otimes k}A(U^\dagger)^{\otimes k}] \\ &= \int_{U(d)} U^{\otimes k}A(U^\dagger)^{\otimes k} d\mu(U). \end{aligned} \quad (137)$$

If we have an expression for the *kth moment operator* for the Haar measure $\mu_{U(d)}$, we can calculate the expectation value of arbitrary polynomials $p_k(U, U^\dagger)$ over $U \sim \mu_{U(d)}$ by a linear contraction, Eq. (136).

The crucial property that characterizes the *kth moment operator* of $\mu_{U(d)}$ is the following: consider a fixed unitary $U \in U(d)$ then a short calculation exploiting the unitary invariance of the Haar measure reveals that

$$U^{\otimes k} \mathcal{M}_{\mu_{U(d)}}^{(k)}(A) = \mathcal{M}_{\mu_{U(d)}}^{(k)}(A)U^{\otimes k}. \quad (138)$$

We find that $\mathcal{M}_{\mu_{U(d)}}^{(k)}(A)$ commutes with every unitary U raised to the *kth tensor power*.

For a set of endomorphisms $\mathcal{A} \subset L(W)$ on a vector space W one calls the set

$$\text{comm}(\mathcal{A}) = \{B \in L(W) \mid BA = AB \quad \forall A \in \mathcal{A}\} \quad (139)$$

of all endomorphisms that commute with all elements of \mathcal{A} the *commutant* of \mathcal{A} . The following lemma establishes that not only does $\mathcal{M}_{\mu_{U(d)}}^{(k)}(A)$ commute with every unitary of the form $U^{\otimes k}$ but it is in fact the orthogonal projector onto the commutant of $\mathcal{A} = \{U^{\otimes k} \mid U \in U(d)\}$, where orthogonality is understood with respect to the Hilbert-Schmidt inner product, Eq. (1). As becomes motivated shortly, we refer to

$$\Delta^{(k)} : U(d) \rightarrow U(d^k), \quad U \mapsto U^{\otimes k} \quad (140)$$

as the *diagonal representation* of $U(d)$.

Lemma 29 (*kth moment operator*): The *kth moment operator* $\mathcal{M}_{\mu_{U(d)}}^{(k)}$ is the orthogonal projector onto $\text{comm}\{\Delta^k[U(d)]\}$, the commutant of the *k-order diagonal representation* of $U(d)$.

Proof. With Eq. (138) we establish that the range of $\mathcal{M}_{\mu_{U(d)}}^{(k)}$ is in $\text{comm}\{\Delta^k[U(d)]\}$. The converse also holds since for $A \in \text{comm}\{\Delta^k[U(d)]\}$ we calculate that $\mathcal{M}_{\mu_{U(d)}}^{(k)}(A) = A\mathcal{M}_{\mu_{U(d)}}^{(k)}(\mathbb{1}) = A$. Thus, it remains to check the orthogonality $[\mathcal{M}_{\mu_{U(d)}}^{(k)}]^\dagger = \mathcal{M}_{\mu_{U(d)}}^{(k)}$. The orthogonality requirement follows in very few lines of calculation using linearity and cyclicity of the trace. ■

Note that the argument of the proof applies more generally and yields the analogous result for arbitrary groups equipped with a Haar measure, e.g., the uniform measure on a finite group.

The commutant of the diagonal representation of the unitary group can be characterized using a powerful result from representation theory: Schur-Weyl duality. To set the stage for explaining the result we start by reviewing some basic definitions and results from representation theory.

1. Representation theory

Let us start with the most basic definitions. For a proper introduction we refer to Simon’s book [52] and to Goodman and Wallach’s book [53] for the representation theory of the standard matrix groups.

Let G and H be groups.

(i) $f : G \rightarrow H$ is a (*group*) *homomorphism* if $f(g_1g_2) = f(g_1)f(g_2)$ for all $g_1, g_2 \in G$. Note that this condition implies that $f(e_G) = e_H$ and $f(g^{-1}) = f(g)^{-1}$ for all $g \in G$.

(ii) A homomorphism $R : G \rightarrow GL(V)$ into the invertible operators on a vector space V is called a *linear (group) representations*. R is a *unitary representation* if $R : G \rightarrow U(\mathcal{H})$ is a homomorphism to a unitary group $U(\mathcal{H}) \subset L(\mathcal{H})$ on some Hilbert space. We are concerned only with such unitary representations and, hence, often omit the word “unitary.”

(iii) A subspace $V \subset \mathcal{H}$ is said to be *invariant* if $R(g)V \subseteq V$ for all $g \in G$. R is called *irreducible* if the only invariant subspaces are $\{0\}$ and \mathcal{H} itself. *Irreducible representations* are also called *irreps* for short.

(iv) Two representations $R : G \rightarrow U(\mathcal{H})$ and $\tilde{R} : G \rightarrow U(\tilde{\mathcal{H}})$ are said to be *unitarily equivalent* if there is a unitary operator $W : \mathcal{H} \rightarrow \tilde{\mathcal{H}}$ such that $\tilde{R}(g) = WR(g)W^\dagger$ for all $g \in G$.

If $R_i : G \rightarrow \mathcal{H}_i$ for $i = 1, 2$ are two representations of G then $(R_1 \oplus R_2)(g) := R_1(g) \oplus R_2(g)$ defines another representation $R_1 \oplus R_2 : G \rightarrow \mathcal{H}_1 \oplus \mathcal{H}_2$. This representation has \mathcal{H}_1 and \mathcal{H}_2 as invariant subspaces. Conversely, if a

representation R has a nontrivial invariant subspace V then it can be decomposed as $R = R|_V \oplus R|_{V^\perp}$. By iterating this insight, we have the following statement (see, e.g., [52, Theorem II.2.3]).

Proposition 30 (Decomposition into irreps): Let $R : G \rightarrow L(\mathcal{H})$ be a unitary representation of a group G on a finite-dimensional Hilbert space \mathcal{H} . Then (R, \mathcal{H}) can be decomposed into a direct sum of irreps (R_i, \mathcal{H}_i) of G as

$$\mathcal{H} = \bigoplus_i \mathcal{H}_i \quad \text{and} \quad R(g) = \bigoplus_i R_i(g). \quad (141)$$

Several irreps R_{i_1}, \dots, R_{i_m} in the decomposition, Eq. (141), might be unitarily equivalent to each other. The maximum number m is called the *multiplicity* of that irrep. The space \mathbb{C}^m in the resulting identification

$$\bigoplus_{j=1}^m R_{i_j}(g) \cong R_{i_1}(g) \otimes \mathbb{1}_m \in L(\mathcal{H}_1 \otimes \mathbb{C}^m) \quad (142)$$

is called the *multiplicity space* of R_{i_1} . The decomposition, Eq. (141), is called *multiplicity-free* if all irreps R_i are inequivalent, i.e., not isomorphic.

Theorem 31 (Schur's lemma): Let $R : G \rightarrow U(\mathcal{H})$ be an irrep of G on \mathcal{H} . If $A \in L(\mathcal{H})$ satisfies

$$AR(g) = R(g)A \quad \forall g \in G \quad (143)$$

then $A = c\mathbb{1}$ for some $c \in \mathbb{C}$.

Proof. The condition, Eq. (143), implies that $R(h)A^\dagger = A^\dagger R(h)$ for all $h = g^{-1} \in G$. Hence, this condition also holds for $\text{Re}(A) := \frac{1}{2}(A + A^\dagger)$ and $\text{Im}(A) := 1/2i(A - A^\dagger)$ and A is a constant if they both are. Hence, it is sufficient to prove the theorem for $A \in \text{Herm}(\mathcal{H})$.

Let $|\psi\rangle$ be an eigenvector with $A|\psi\rangle = \lambda|\psi\rangle$ and $\text{Eig}_\lambda(A) := \{|\psi\rangle : A|\psi\rangle = \lambda|\psi\rangle\}$ the full eigenspace. Then $R(g)|\psi\rangle \in \text{Eig}_\lambda(A)$ for all $g \in G$ because $AR(g)|\psi\rangle = R(g)A|\psi\rangle = \lambda R(g)|\psi\rangle$. So, $\text{Eig}_\lambda(A)$ is an invariant subspace. Since $\text{Eig}_\lambda(A) \neq \{0\}$ and R is an irrep, $\text{Eig}_\lambda(A) = \mathcal{H}$ follows. ■

Corollary 32 (Irreps of Abelian groups): If G is Abelian then every irrep has dimension 1.

Proof. Let R be an irrep of G on \mathcal{H} . Theorem 31 implies that each $g \in G$ has representation $R(g) = c_g\mathbb{1}$ for some constant c_g . Hence, every subspace of \mathcal{H} is invariant under R . Since R is an irrep this is only possible if $\dim(\mathcal{H}) = 1$. ■

There is also a slightly more general version of Schur's lemma.

Theorem 33 (Schur's lemma II): Let $R : G \rightarrow U(\mathcal{H})$ and $\tilde{R} : G \rightarrow U(\tilde{\mathcal{H}})$ be two irreps of G on finite-dimensional Hilbert spaces \mathcal{H} and $\tilde{\mathcal{H}}$. If $A \in L(\mathcal{H}, \tilde{\mathcal{H}})$

satisfies

$$AR(g) = \tilde{R}(g)A \quad \forall g \in G \quad (144)$$

then either $A = 0$ or R_1 and R_2 are unitarily equivalent up to a constant factor.

Proof. The condition, Eq. (144), implies that for all $g \in G$

$$R(g)A^\dagger = A^\dagger\tilde{R}(g) \quad (145)$$

and, hence,

$$R(g)A^\dagger A = A^\dagger AR(g), \quad (146)$$

$$\tilde{R}(g)AA^\dagger = AA^\dagger\tilde{R}(g). \quad (147)$$

Schur's lemma (Theorem 31) implies that $A^\dagger A = c\mathbb{1}$ and $AA^\dagger = \tilde{c}\mathbb{1}$ for constants c, \tilde{c} . Obviously, $c = \tilde{c}$, the eigenvalues of both operators have to coincide. Either $c = 0$ so that $A = 0$ or $W = A/\sqrt{c}$ is a unitary. In the latter case

$$WR(g) = \tilde{R}(g)W \quad (148)$$

for all $g \in G$, i.e., R and \tilde{R} are unitarily equivalent. ■

A unitary W relating two representations R and \tilde{R} as in Eq. (148) is called an *intertwining* unitary of R and \tilde{R} .

2. Schur-Weyl duality and the commutant of the diagonal action

To calculate the moments of random variables depending on Haar random unitaries, we are interested in understanding the commutant of the diagonal representation of the unitary group. Formally, we define the diagonal representation of $U(d)$ on $(\mathbb{C}^d)^{\otimes k}$ as

$$\Delta_d^k : U(d) \rightarrow U[(\mathbb{C}^d)^{\otimes k}] \quad (149)$$

by linearly extending the action

$$\Delta_d^k(U)(|\psi_1\rangle \otimes \dots \otimes |\psi_k\rangle) := (U|\psi_1\rangle) \otimes \dots \otimes (U|\psi_k\rangle). \quad (150)$$

The representation Δ_d^k has a duality relation with another well-known representation on \mathbb{C}^k : the representation π_k of the *symmetric group* \mathcal{S}_k permuting the k tensor components:

$$\begin{aligned} \pi_k : \mathcal{S}_k &\rightarrow U[(\mathbb{C}^d)^{\otimes k}], \\ \pi_k(\sigma) [|\psi_1\rangle \otimes \dots \otimes |\psi_k\rangle] &:= |\psi_{\sigma^{-1}(1)}\rangle \otimes \dots \otimes |\psi_{\sigma^{-1}(k)}\rangle. \end{aligned} \quad (151)$$

We note that $\pi_k(\sigma)$ and $\Delta_d(U)$ commute for any $\sigma \in \mathcal{S}_k$ and $U \in U(d)$.

Let us consider the following two irreducible representations of the symmetric group, which appear in the decomposition, Proposition 30, of π_k for any k . We call $|\Psi\rangle \in (\mathbb{C}^d)^{\otimes k}$ *symmetric* if $\pi_k(\sigma)|\Psi\rangle = |\Psi\rangle$ for all $\sigma \in \mathfrak{S}_k$ and *antisymmetric* if $\pi_k(\sigma)|\Psi\rangle = \text{sign}(\sigma)|\Psi\rangle$ for all $\sigma \in \mathfrak{S}_k$. The *symmetric subspace* $\mathcal{H}_{\text{sym}^k}$ and *antisymmetric subspace* \mathcal{H}_{\wedge^k} of $(\mathbb{C}^d)^{\otimes k}$ are the subspaces consisting of all symmetric and all antisymmetric vectors, respectively.

Lemma 34 (Symmetric subspace): (i) The dimension of the symmetric subspace $P_{\text{sym}^k}(\mathbb{C}^d)^{\otimes k}$ is

$$\text{Tr}[P_{\text{sym}^k}] = \binom{k+d-1}{d-1}. \quad (152)$$

(ii) The orthogonal projectors onto the symmetric and antisymmetric subspace are

$$P_{\text{sym}^k} = \frac{1}{k!} \sum_{\sigma \in \mathfrak{S}_k} \pi_k(\sigma)$$

and $P_{\wedge^k} = \frac{1}{k!} \sum_{\sigma \in \mathfrak{S}_k} \text{sign}(\sigma) \pi_k(\sigma), \quad (153)$

respectively.

Proof. The first statement is a combinatorial one. The trace of the symmetric projector is the number of ways to distribute k indistinguishable particles (bosons) into d boxes (modes), i.e., the dimension of the corresponding subspace of the bosonic subspace, which is known to be given by the binomial coefficient.

The second statement follows, e.g., for P_{sym^k} by realizing that any symmetric vector in the range of P_{sym^k} and that this operator is indeed a projector, i.e., that P_{sym^k} is self-adjoint and $P_{\text{sym}^k} P_{\text{sym}^k} = P_{\text{sym}^k}$. ■

For the case of $k = 2$ the decomposition into these two subspaces is very familiar. It is easy to see that any matrix can be decomposed into a symmetric and an antisymmetric part, which are orthogonal to each other. This implies that

$$(\mathbb{C}^d)^{\otimes 2} = \mathcal{H}_{\text{sym}^2} \oplus \mathcal{H}_{\wedge^2}. \quad (154)$$

Note that due to Corollary 32, both the symmetric and the antisymmetric subspace are isomorphic to $\mathbb{C}^{m_{\text{sym}^2}}$ and $\mathbb{C}^{m_{\wedge^2}}$, respectively. Here m_{sym^2} and m_{\wedge^2} are the multiplicities of the two distinct one-dimensional irreps of \mathfrak{S}_2 .

For $k > 2$ there is a similar decomposition with more summands called *Schur-Weyl decomposition*. The Schur-Weyl decomposition relies on a duality relation between the commuting representations Δ_d^k and π_k . The representations Δ_d^k and π_k span each other's commutant as algebras.

Theorem 35 (Schur-Weyl duality [53, Theorem 4.2.10]): For the two commuting representations, Eqs. (151) and (150), it holds that

$$\text{comm} \{ \Delta_d^k[U(d)] \} = \text{span} [\pi_k(\mathfrak{S}_k)] \quad (155)$$

and

$$\text{comm} [\pi_k(\mathfrak{S}_k)] = \text{span} \{ \Delta_d^k[U(d)] \}. \quad (156)$$

By Schur's lemma such a duality relation implies that the multiplicity spaces of the irreducible representation of one representation are irreducible representations of the dual representation and vice versa. In other words, \mathbb{C}^d decomposes into multiplicity-free representations of the combined action $U(d) \times \mathfrak{S}_k$. In order to state this composition, we write $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_{l(\lambda)}) \vdash k$ for a partition of k into $l(\lambda)$ nonincreasing integers with $\lambda_1 \geq 1$ and fulfilling

$$k = \sum_{i=1}^{l(\lambda)} \lambda_i. \quad (157)$$

Such partitions of integers label the irreducible representations of the symmetric group and the diagonal representation. As a consequence of Schur-Weyl duality one can prove.

Theorem 36: (Schur-Weyl decomposition [53, Theorem 9.1.2]): The action of $U(d) \times \mathfrak{S}_k$ on $(\mathbb{C}^d)^{\otimes k}$ given by the commuting representations, Eqs. (151) and (150), is multiplicity-free and $(\mathbb{C}^d)^{\otimes k}$ decomposes into irreducible components as

$$(\mathbb{C}^d)^{\otimes k} \cong \bigoplus_{\lambda \vdash k, l(\lambda) \leq d} W_\lambda \otimes S_\lambda, \quad (158)$$

where $U(d)$ acts nontrivially only on W_λ and \mathfrak{S}_k acts nontrivially only on S_λ . For any $k \geq 2$, both $\mathcal{H}_{\text{sym}^k}$ and \mathcal{H}_{\wedge^k} occur as components in the direct sum, Eq. (158).

The spaces W_λ are called *Weyl modules* and S_λ *Specht modules*. Schur-Weyl duality implies that the Weyl modules are the multiplicity spaces of the irreps of \mathfrak{S}_k and, similarly, the Specht modules are the multiplicity spaces of the irreps of $U(d)$.

Schur-Weyl duality, Theorem 35, and the resulting decomposition, Theorem 36, give a simple characterization of the commutant of the diagonal action. The relation, Eq. (155), allows one to derive an expression for the k -moment operator $\mathcal{M}_{\mu_{U(d)}}^{(k)}$ as the orthogonal projector onto the span of the symmetric group. But one has to be careful since $\{ \pi_k^d(\sigma) \}_{\sigma \in \mathfrak{S}_k}$ is not an orthonormal basis. Note that it only becomes an orthogonal set asymptotically for large k , which can be exploited in some applications, e.g., Ref. [54]. A general expression in terms of so-called

Weingarten functions [55] was derived by Collins and Sniday [56], see also the Supplemental Material of Ref. [57] for a convenient expression of their result and a summary of the derivation. For our purposes we only need to derive an expression $\mathcal{M}_{\mu_{U(d)}}^{(k)}$ for certain special cases, namely, for $k = 2$ and when restricted to symmetric endomorphisms as its input.

We begin with the second moment, $k = 2$.

Proposition 37 (Second-moment operator): For an operator $A \in L(\mathbb{C}^d \otimes \mathbb{C}^d)$, $d \geq 2$, it holds that

$$\mathcal{M}_{\mu_{U(d)}}^{(2)}(A) = c_{\text{sym}^2} P_{\text{sym}^2} + c_{\wedge^2} P_{\wedge^2}, \quad (159)$$

with $c_{\text{sym}^2} = 2/[d(d+1)]\text{Tr}[AP_{\text{sym}^2}]$ and $c_{\wedge^2} = 2/[d(d-1)]\text{Tr}[AP_{\wedge^2}]$.

Proof. From Lemma 29 and Theorem 35 we know that $\mathcal{M}_{\mu_{U(d)}}^{(2)}(A)$ is a linear combination of the identity $\mathbb{1}$ and the swap operator \mathbb{F} from Eq. (6). For \mathfrak{S}_2 the expansion of the projectors onto the symmetric and antisymmetric subspace, Eq. (153), can be inverted yielding $\text{id} = P_{\text{sym}^2} + P_{\wedge^2}$ and $\mathbb{F} = P_{\text{sym}^2} - P_{\wedge^2}$. This establishes the form of Eq. (159). Since P_{sym^2} and P_{\wedge^2} are mutually orthogonal projectors and $\mathcal{M}_{\mu_{U(d)}}^{(2)}$ is an orthogonal projector the coefficients are given by $c_{\text{sym}^2} = \text{Tr}[AP_{\text{sym}^2}]/\text{Tr}[P_{\text{sym}^2}] = \{2/[d(d+1)]\}\text{Tr}[AP_{\text{sym}^2}]$ and c_{\wedge^2} analogously. ■

Second, we allow for arbitrary k but restrict the input of $\mathcal{M}_{\mu_{U(d)}}^{(k)}$ to endomorphisms that are itself symmetric, i.e., of product form. In this case we also find an orthogonal decomposition as given by the following lemma.

Lemma 38 (Moment operator on symmetric operators): For any operator $A \in L(\mathbb{C}^d)$ it holds that

$$\mathcal{M}_{\mu_{U(d)}}^{(k)}(A^{\otimes k}) = \sum_{\lambda \vdash k, l(\lambda) \leq d} c_{\lambda} P_{\lambda}, \quad (160)$$

with P_{λ} the orthogonal projector onto $W_{\lambda} \otimes S_{\lambda}$ and $c_{\lambda} = \text{Tr}[P_{\lambda} A^{\otimes k}]/\text{Tr}[P_{\lambda}]$. Furthermore, if the operator A is of *unit rank*, then

$$\mathcal{M}_{\mu_{U(d)}}^{(k)}(A^{\otimes k}) = c P_{\text{sym}^k}, \quad (161)$$

with $c = \text{Tr}[P_{\text{sym}^k} A^{\otimes k}]/\text{Tr}[P_{\text{sym}^k}]$.

Proof. We fix some $A \in L(\mathbb{C}^d)$ and denote $E := \mathcal{M}_{\mu_{U(d)}}^{(k)}(A^{\otimes k})$. By the definition of the moment operator, Eq. (137), $E = \int_{U(d)} (UAU^{\dagger})^{\otimes k} d\mu_{U(d)}(U)$ and it becomes apparent that E commutes with $\pi_k^d(\sigma)$ for any $\sigma \in \mathfrak{S}_k$. In other words, $E \in \text{comm}\Delta_k^d[U(d)] \cap \text{comm}\pi_k^d(\mathfrak{S}_k)$ by Lemma 29. By Schur's lemma (Theorem 31) and the Schur-Weyl decomposition, Eq. (158), we thus conclude that E acts proportionally to the identity on every Weyl module W_{λ} and Specht module S_{λ} . Denoting the orthogonal projector

onto $W_{\lambda} \otimes S_{\lambda}$ as P_{λ} , the operator E permits the decomposition $E = \sum_{\lambda \vdash k, l(\lambda) \leq d} c_{\lambda} P_{\lambda}$ with $c_{\lambda} \in \mathbb{C}$. Since the projectors are onto mutually orthogonal the coefficients are given by $c_{\lambda} = \text{Tr}[A^{\otimes k} P_{\lambda}]/\text{Tr}[P_{\lambda}]$. This establishes the lemma's first assertion for E .

Finally, for unit rank A , i.e., $A = |\psi\rangle\langle\psi|$ with $|\psi\rangle, |\phi\rangle \in \mathbb{C}^d$, we observe that $P_{\text{sym}^k} A^{\otimes k} P_{\text{sym}^k} = P_{\text{sym}^k} |\psi\rangle^{\otimes k} \langle\psi|^{\otimes k} P_{\text{sym}^k} = A^{\otimes k}$. Hence, $c_{\lambda} = 0$ for all λ that do not correspond to the symmetric subspace. This leaves us with the lemma's second expression for E and unit rank A . ■

3. Uniformly random state vectors

One can also define a uniform distributed on pure quantum states in multiple equivalent ways. First, one can draw randomly from the complex sphere $\mathbb{S}(\mathbb{C}^d)$, i.e., the set of normalized vectors in \mathbb{C}^d . Indeed, there is a unique uniform probability measure $\mu_{\mathbb{S}(\mathbb{C}^d)}$ on $\mathbb{S}(\mathbb{C}^d)$ that is invariant under the canonical action of $U(d)$ on \mathbb{C}^d . By definition we see that a column $|\psi\rangle = U|0\rangle$ of a Haar randomly drawn unitary $U \sim \mu_{U(d)}$ is distributed according to $\mu_{\mathbb{S}(\mathbb{C}^d)}$. Finally, we can switch to density matrices by factoring out a global phase. In more detail, the *complex projective space* $\mathbb{C}\mathbf{P}^{d-1} := \mathbb{S}(\mathbb{C}^d)/U(1)$ is the set of state vectors modulo a phase in $U(1)$, which can be identified with the set of pure density matrices $\mathbb{C}\mathbf{P}^{d-1} \subset \mathcal{S}(\mathbb{C}^d)$. It also has a uniform unitarily invariant probability distribution: a uniformly random pure state $|\psi\rangle\langle\psi|$ can be obtained by drawing $|\psi\rangle \sim \mu_{\mathbb{S}(\mathbb{C}^d)}$.

We can calculate the moments of polynomials that depend on states drawn uniformly from $\mu_{\mathbb{S}(\mathbb{C}^d)}$ using the moment operator $\mathcal{M}_{\mu_{U(d)}}^{(k)}$. To this end, note that any polynomial $p_k(|\psi\rangle, \langle\psi|)$ of degree k in the component of each $|\psi\rangle$ and $\langle\psi|$ can be written as a contraction of $|\psi\rangle\langle\psi|^{\otimes k}$ with some operator in $L(\mathbb{C}^{d^k})$. For this reason the following lemma summarizes everything we need.

Lemma 39 (Moment operator of random states): Let $K_{\mu_{\mathbb{S}(\mathbb{C}^d)}}^{(k)}$ be the moment operator for $|\psi\rangle \sim \mu_{\mathbb{S}(\mathbb{C}^d)}$ explicitly defined by

$$K_{\mu_{\mathbb{S}(\mathbb{C}^d)}}^{(k)} := \int_{\mathbb{S}(\mathbb{C}^d)} (|\psi\rangle\langle\psi|)^{\otimes k} d\mu_{\mathbb{S}(\mathbb{C}^d)}(\psi). \quad (162)$$

It holds that

$$K_{\mu_{\mathbb{S}(\mathbb{C}^d)}}^{(k)} = \frac{k!(d-1)!}{(k+d-1)!} P_{\text{sym}^k}, \quad (163)$$

where P_{sym^k} is the projector, Eq. (153), onto the symmetric subspace.

Proof. As $\mu_{\mathbb{S}(\mathbb{C}^d)}$ is $U(d)$ invariant, we find $K_k = \mathcal{M}_{\mu_{U(d)}}^{(k)}[(|\psi\rangle\langle\psi|)^{\otimes k}]$. Lemma 38 thus implies that $K_k = c P_{\text{sym}^k}$ with

$$c = \frac{\text{Tr}[P_{\text{sym}^k}(|\psi\rangle\langle\psi|)^{\otimes k}]}{\text{Tr}[P_{\text{sym}^k}]}.$$

Since P_{sym^k} acts trivially on $|\psi\rangle$ and it is normalized, the enumerator evaluates to 1. The denominator is the dimension of P_{sym^k} given by Eq. (152). ■

4. Unitary, spherical, and complex-projective k -designs

With our excursion to representation theory we derived expressions to calculate the moments of random variables on uniformly random states and unitaries. The very same results can also be used for certain other interesting probability distributions. To this end, note that if we want to control only the first moments of a random variable that is a polynomial of degrees ℓ in a random state or unitary, then our calculation will only involve the moment operators $\mathcal{M}_{\mu_{U(d)}}^{(k)}$ for $k \leq t\ell$. In many applications it is sufficient to control the expectation value and the variance of low-degree polynomials. In these cases, any probability distribution that reproduces the first couple of moments of the uniform distributions can be used without changing the mathematical expressions. This idea is formalized by the definition of k -designs.

Definition 40 (Unitary k -design): A distribution μ on the unitary group $U(d)$ is a *unitary k -design* if its k th moment operator, Eq. (137), coincides with the one of the Haar measure,

$$\mathcal{M}_{\mu}^{(k)} = \mathcal{M}_{\mu_{U(d)}}^{(k)}. \quad (164)$$

Furthermore, a subset $\{U_1, \dots, U_{n_{\mathbb{C}}}\} \subset U(d)$ is called a *unitary k -design* if its uniform distribution is 1.

Note that by definition, any unitary k -design is also a unitary $(k - 1)$ -design for $k \geq 2$.

A famous example of a unitary design in the context of quantum computing is the Clifford group. The n -qubit *Clifford group* $Cl_n \subset U(2^n)$ is the normalizer of the Pauli group \mathcal{P}_n (see Sec. 75),

$$Cl_n := \{U \in U(2^n) : U\mathcal{P}_n U^\dagger \subset \mathcal{P}_n\}. \quad (165)$$

The n -qubit Clifford group is generated by the single qubit Hadamard gate H and the phase gate S given by (see, e.g., [58, Theorem 10.6])

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 1 & \\ & i \end{pmatrix} \quad (166)$$

together with the two-qubit CNOT gate

$$\text{CNOT} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x \quad (167)$$

acting locally on any qubit.

Together with the $T = \sqrt{S}$ gate the Clifford group is a universal gate set (see, e.g., [58, Sec. 4.5.3]).

The Clifford group is a unitary 3-design but not a unitary 4-design [59–61]. Being a subgroup of the unitary group the commutant of the diagonal action of the Clifford group for $k > 3$ is, thus, a strictly larger space than the span of the permutation group. A classification of the “missing generators” of the commutant was done by Gross *et al.* [62].

Analogously to unitary designs, we can define spherical k -designs. For a distribution μ on the complex sphere $\mathbb{S}(\mathbb{C}^d)$ we define the k th *moment operator* as

$$K_{\mu}^{(k)} := \int_{\mathbb{S}(\mathbb{C}^d)} (|\psi\rangle\langle\psi|)^{\otimes k} d\mu(\psi). \quad (168)$$

Definition 41: (Complex spherical and projective k -design): A distribution μ on $\mathbb{S}(\mathbb{C}^d)$ is a *spherical k -design* if

$$K_{\mu}^{(k)} = K_{\mu_{U(d)}}^{(k)}. \quad (169)$$

Furthermore, a subset $\mathbb{S}(\mathbb{C}^d)$ is called a *spherical k -design* if its uniform distribution is 1. The corresponding distribution of $|\psi\rangle\langle\psi|$ is called a *complex projective k -design*.

See also Refs. [63,64] for related definitions.

Analogously to the relation of the uniform measure on $U(d)$ and $\mathbb{S}(\mathbb{C}^d)$, a rather obvious but important example of a spherical k -design is the orbit of a unitary k -design. If μ is a unitary k -design for $U(d)$ and $|\psi\rangle \in \mathbb{C}^d$ then the induced distribution $\tilde{\mu}$ given by $U|\psi\rangle$ with $U \sim \mu$, is a complex spherical k -design.

One can use this relation to see that the Clifford group being a unitary 3-design implies the analogous statement for stabilizer states. The set of all stabilizer states, Eq. (75), is known to be a 2-design [65,66], actually even a 3-design but not a 4-design [59,60,67].

Other examples for spherical designs that play important roles in quantum system characterization are *mutually unbiased bases* and *symmetric, informationally complete POVMs*.

Mutually unbiased bases (MUBs) are sets of bases with minimal overlaps. More explicitly, two orthonormal bases $\{|\psi_i\rangle\}_{i \in [d]} \subset \mathbb{C}^d$ and $\{|\phi_i\rangle\}_{i \in [d]} \subset \mathbb{C}^d$ are said to be *mutually unbiased* if $|\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{d}$ for all $i, j \in [d]$. For instance, if $U \in U(d)$ is the discrete Fourier transform then the bases $\{|i\rangle\}_{i \in [d]} \subset \mathbb{C}^d$ and $\{U|i\rangle\}_{i \in [d]} \subset \mathbb{C}^d$ are mutually unbiased. The number of MUBs in \mathbb{C}^d is upper bounded by $d + 1$ and, in prime power dimensions (e.g., for qubits), there are exactly $d + 1$ MUBs [68,69]. However, it is a well-known open problem to exactly obtain this number for all d . Klappenecker and Roettler [70] showed that maximal sets of MUBs are complex spherical 2-designs.

A *symmetric, informationally complete (SIC) POVM* is given by a set of d^2 normalized vectors $\{|\psi_j\rangle\}_{j \in [d^2]} \subset \mathbb{S}(\mathbb{C}^d) \subset \mathbb{C}^d$ satisfying

$$|\langle \psi_i | \psi_j \rangle|^2 = \frac{1}{d+1} \quad \forall i \neq j. \quad (170)$$

“Symmetric” refers to the inner products being all equal. Zauner [71] has investigated SIC POVMs systematically. Renes *et al.* [72] have shown that SIC POVMs are indeed 2-designs. Both works provide explicit constructions for small dimensions.

J. Shadow-fidelity estimation

Another recently proposed approach to fidelity estimation makes use of estimating so-called classical shadows [20,21]. The principle idea of shadow estimation is to calculate the least-squares estimator of a quantum state from recorded classical measurement outcomes with measurement setting drawn from a certain *measurement frame*. As we see in this section such a POVM that allows for a quite explicit analysis is given by a complex projective 3-design.

From the state’s least-squares estimator one can construct estimators of multiple target functions of the state, which are linear functions or even higher polynomials. The sampling complexity of the derived estimators can be captured by a so-called *shadow norm* that is defined in terms of the measurement frame. The classical post-processing complexity is determined by the complexity of constructing the state estimator and evaluating the target functions. Operationally, the analyzed POVM measurement is assumed to be implementable by random unitaries from a suitable ensemble and a consecutive basis measurement. While shadow estimation is a rather broad and flexible framework, we focus on the estimation of *fidelities with pure target states* using unitaries that form a unitary 3-design, e.g., multiqubit Clifford gates or suitable subgroups thereof. Besides being an instructive example for shadow-fidelity estimation, the 3-design setting can be equipped with a performance guarantees that features a sampling complexity $O(\epsilon^{-2})$ that does not scale with the Hilbert space dimension. This system-size-independent scaling is not achievable in general for other measurement frames.

The complete shadow-fidelity estimation (SFE) protocol is the following.

Protocol 42 (SFE): Let μ be a distribution on $U(d)$, $\{|b\rangle : b \in [d]\} \subset \mathbb{C}^d$ an orthonormal basis and $\rho \in \mathcal{S}(\mathbb{C}^d)$ be a target state.

The protocol consists of the following steps applied to state preparations $\{\tilde{\rho}_i\}_{i=1}^{n_{\tilde{\rho}}} \subset \mathcal{S}(\mathbb{C}^d)$. For each $\tilde{\rho}_i$ perform the following steps.

- (i) Draw $U_i \sim \mu$.
- (ii) Perform the following experiment:

- (I) Prepare $\tilde{\rho}_i$.
- (II) Apply the gate $\tilde{\rho}_i \mapsto U_i \tilde{\rho}_i U_i^\dagger$.
- (III) Perform the basis measurement \mathcal{B} and record the outcome $b_i \in \{0, 1\}^n$.
- (iii) Calculate

$$\hat{f}_i = (d+1) \langle b_i | U_i \rho U_i^\dagger | b_i \rangle - 1. \quad (171)$$

Output the median of means estimator, Eq. (26), of $\{\hat{f}_i\}_{i=1}^{n_{\tilde{\rho}}}$.

We present the protocol as iterations over combined experimental and classical pre- and postprocessing steps. Note, however, that one can complete the three stages separately: first one can classically generate the complete sequence of $n_{\tilde{\rho}}$ random unitaries. Then, one can subsequently perform the quantum experiment, i.e., all repetitions of step (ii). Importantly, at this stage not even the knowledge of the target state ρ is required. Storage of the experimental outcomes, $n_{\tilde{\rho}}$ bit strings, requires $n_{\tilde{\rho}} \log n$ bits. These bit strings together with a prescription of the random sequence of unitaries are then taken as the input of the postprocessing algorithm that calculates the median of means estimator. The complexity the classical postprocessing depends on the complexity of calculating the overlap of Eq. (171). For an arbitrary target state ρ the effort of performing this task can scale exponentially in the number of qubits. In contrast, for stabilizer states and Clifford group unitaries the Gottesman-Knill theorem, see, e.g., Ref. [58], allows for an efficient computation of the expression.

Shadow-fidelity estimation comes with the following guarantee.

Theorem 43 (Guarantee for SFE): Consider Protocol 42 with μ being a unitary 3-design and ρ a *pure* target state. Choose $\delta \in (0, 1)$, $\epsilon > 0$ and a number

$$n_{\tilde{\rho}} \geq 160 \frac{1}{\epsilon^2} \ln \frac{1}{\delta} \quad (172)$$

such that it is a multiple of $k = \lceil 8 \ln(1/\delta) \rceil$. Then, the median of means estimator of the protocol is an ϵ -accurate unbiased estimator of $F(\rho, \tilde{\rho})$ with confidence $1 - \delta$ for $n_{\tilde{\rho}}$ i.i.d. state preparations; the median is taken over $l = n_{\tilde{\rho}}/k$ means, each of which is an empirical mean of k realizations of \hat{f}_i .

Theorem 43 shows that SFE requires a number of state copies that for arbitrary pure target states does not depend on the Hilbert space dimension.

With the DFE protocol of Sec. IIH we already encountered another fidelity estimation protocol. In contrast to SFE, recall that DFE features a sampling complexity independent of the Hilbert space dimension only for the class of well-conditioned states, cmp. Theorem 27. Keep in mind, however, that in order to additionally ensure an efficient classical postprocessing also SFE requires further structure such as provided by stabilizer states. Finally, note that

SFE and DFE, as presented here, make use of a different type of measurement data. While SFE uses basis measurement randomly selected from a large set of bases, DFE uses the expectation values of observables. Correspondingly, they differ in their requirements for experimentally implementations.

The proof of the performance guarantee, Theorem 43, proceeds in three steps: first, we have to establish that the SFE estimator actually estimates the fidelity for pure target states. To derive the sampling complexity of the estimator a natural attempt would be to employ Hoeffding’s inequality. Unfortunately, the random variables \hat{f}_i defined in Eq. (171) only have bounds scaling as $O(d)$. This becomes exponentially large in the number of qubits and does not yield the desired scaling. The main insight underlying the efficiency of shadow-fidelity estimation is that due to the structure of the unitary 3-design the variance of \hat{f}_i is still bounded in $O(1)$. Thus, as a second step we derive the bound for the variance. Finally, by combining both results we arrive at the sampling complexity using the tail bound for the median of mean estimator introduced in Theorem 9. Using the median of mean estimator allows us to derive a sampling complexity in $O(\ln \delta^{-1})$ in the confidence. Note that simply using a mean estimator in the SFE protocol can also be equipped with a guarantee with sampling complexity in $O(\delta^{-1})$ using Chebyshev’s inequality, Theorem 7. A mean estimator might in a practical parameter regime even be more precise compared to the median of mean estimator.

Lemma 44 (Unbiasedness of SFE estimator): Consider Protocol 42 with μ being a unitary 2-design and ρ a pure target state. Let \hat{f}_i be a random variable, Eq. (171), with respect to a state preparation $\tilde{\rho}$. Then

$$\mathbb{E}[\hat{f}_i] = F(\rho, \tilde{\rho}), \quad (173)$$

where the expectation value is taken over both, $U \sim \mu$ and the subsequent random measurement outcome.

Proof. For convenience we suppress writing the index i . Born’s rule for the probability of the measurement outcomes gives us,

$$p(b) = \langle b | U \tilde{\rho} U^\dagger | b \rangle. \quad (174)$$

Thus, the expectation value over U and the measurement reads

$$\begin{aligned} \mathbb{E}[\hat{f}] &= \mathbb{E}_{U \sim \mu} \left\{ \sum_{b=1}^d \langle b | U \tilde{\rho} U^\dagger | b \rangle \right. \\ &\quad \left. \times [(d+1) \langle b | U \rho U^\dagger | b \rangle - 1] \right\}. \end{aligned} \quad (175)$$

The second term can be directly evaluated using the fact that we sum over a basis,

$$\begin{aligned} \sum_{b=1}^d \mathbb{E}_{U \sim \mu} \langle b | U \tilde{\rho} U^\dagger | b \rangle &= \mathbb{E}_{U \sim \mu} [\text{Tr}[U \tilde{\rho} U^\dagger]] \\ &= \text{Tr}[\tilde{\rho}]. \end{aligned} \quad (176)$$

The first term can be calculated using the 3-design property of μ . More precisely, at this point we need only μ to be a 2-design. Recall that if $U \sim \mu$ is a unitary k -design then for any state $|\tau\rangle$ its orbit $|\phi\rangle = U|\tau\rangle$ with the induced measure $\tilde{\mu}$ is a state k -design. Thus, using Eq. (7) and Lemma 39 we calculate that

$$\begin{aligned} &\mathbb{E}_{U \sim \mu} \left[(d+1) \sum_{b=1}^d \langle b | U \tilde{\rho} U^\dagger | b \rangle \langle b | U \rho U^\dagger | b \rangle \right] \\ &= (d+1) \sum_{b=1}^d \text{Tr} \left\{ \mathbb{E}_{U \sim \mu} \left[(U^\dagger |b\rangle \langle b| U)^{\otimes 2} \right] (\tilde{\rho} \otimes \rho) \mathbb{F} \right\} \\ &= (d+1) \sum_{b=1}^d \text{Tr} \left\{ \mathbb{E}_{|\phi\rangle \sim \tilde{\mu}} [(|\phi\rangle \langle \phi|)^{\otimes 2}] (\tilde{\rho} \otimes \rho) \mathbb{F} \right\} \\ &= \text{Tr}[(\mathbb{1} + \mathbb{F})(\tilde{\rho} \otimes \rho) \mathbb{F}] \\ &= \text{Tr}[\rho \tilde{\rho}] + \text{Tr}[\tilde{\rho}] \text{Tr}[\rho]. \end{aligned} \quad (177)$$

Combining both terms again and using that $\text{Tr}[\rho] = 1$, we find that

$$\mathbb{E}[\hat{f}] = \text{Tr}[\rho \tilde{\rho}]. \quad (178)$$

Assuming that ρ is a pure state establishes the statement, Eq. (173). ■

Next we bound the variance.

Lemma 45 (Variance bound for SFE): Consider Protocol 42 with μ being a unitary 3-design and ρ a pure target state. Let \hat{f}_i be a random variable, Eq. (171), with respect to a state preparation $\tilde{\rho}$. Then

$$\text{Var}[\hat{f}_i] < 5, \quad (179)$$

where the variance is taken over both, $U \sim \mu$ and the subsequent random measurement outcome.

Proof. We again suppress the index i . The variance is

$$\text{Var}[\hat{f}] = \mathbb{E}[\hat{f}^2] - \mathbb{E}[\hat{f}]^2. \quad (180)$$

Using Born’s rule Eq. (174), Eq. (176), and that $U|b\rangle$ is distributed as a complex spherical 3-design $\tilde{\mu}$, the second

moment can be written as

$$\begin{aligned} \mathbb{E}[\hat{f}^2] &= d(d+1)^2 \mathbb{E}_{|\phi\rangle \sim \tilde{\mu}} \left\{ \langle \phi | \tilde{\rho} | \phi \rangle | \text{Tr}[\rho |\phi\rangle \langle \phi|] |^2 \right\} \\ &\quad - 2\mathbb{E}[\hat{f}] + \text{Tr}[\tilde{\rho}]. \end{aligned} \quad (181)$$

The first term in this expression can be calculated using the 3-design property of $\tilde{\mu}$ and Lemma 39

$$\begin{aligned} &\mathbb{E}_{|\phi\rangle \sim \tilde{\mu}} \left\{ \langle \phi | \tilde{\rho} | \phi \rangle | \text{Tr}[\rho |\phi\rangle \langle \phi|] |^2 \right\} \\ &= \mathbb{E}_{|\phi\rangle \sim \tilde{\mu}} \left\{ \text{Tr}[\tilde{\rho} |\phi\rangle \langle \phi|] \text{Tr}[\rho |\phi\rangle \langle \phi|] \right\} \\ &= \text{Tr} \left\{ (\tilde{\rho} \otimes \rho \otimes \rho) \mathbb{E}_{|\phi\rangle \sim \tilde{\mu}} [|\phi\rangle \langle \phi|^{\otimes 3}] \right\} \\ &= \frac{6}{d(d+1)(d+2)} \text{Tr} [(\tilde{\rho} \otimes \rho \otimes \rho) P_{\text{sym}^3}]. \end{aligned} \quad (182)$$

We recall that the projector P_{sym^3} onto the symmetric representation of the symmetric group \mathfrak{S}_3 is given by the sum of all six permutations in \mathfrak{S}_3 . Those are the identity, three transpositions, and the cyclic and anticyclic permutation. Writing out this sum and tracking the resulting contractions (which can be most conveniently done using tensor network diagrams) yields

$$\begin{aligned} &\mathbb{E}_{|\phi\rangle \sim \tilde{\mu}} \left\{ \langle \phi | \tilde{\rho} | \phi \rangle | \text{Tr}[\rho |\phi\rangle \langle \phi|] |^2 \right\} \\ &= \frac{1}{d(d+1)(d+2)} (\text{Tr}[\tilde{\rho}] \text{Tr}[\rho]^2 \\ &\quad + 2\text{Tr}[\tilde{\rho}\rho] \text{Tr}[\rho] + \text{Tr}[\tilde{\rho}]\text{Tr}[\rho^2] + 2\text{Tr}[\tilde{\rho}\rho^2]) \\ &= \frac{2 + 4F(\rho, \tilde{\rho})}{d(d+1)(d+2)}, \end{aligned} \quad (183)$$

where we use the normalization of the states and that ρ is pure in the last identity. Combining Eq. (180), (181) and using Eq. (173) from the previous lemma and Eq. (183) we find the upper bound

$$\begin{aligned} \text{Var}[\hat{f}] &= \frac{d+1}{d+2} (2 + 4F) - 2F + 1 - F^2 \\ &< 2(1 + F) + 1 - F^2 \leq 5, \end{aligned} \quad (184)$$

with $F := F(\rho, \tilde{\rho}) \in [0, 1]$. \blacksquare

We have now the ingredients to simply invoke Theorem 9 for the median of mean estimator as the final step.

Proof. By Theorem 9 and the assumptions of Theorem 43 we have for the median of mean estimator $\hat{\mu}$ with confidence $1 - \delta$

$$|\hat{\mu} - \mu| \leq \sigma \sqrt{\frac{32 \ln(1/\delta)}{n_{\tilde{\rho}}}}, \quad (185)$$

where $\mu = \mathbb{E}[\hat{f}_i]$. Now, Eq. (173) implies that $\mu = F(\rho, \tilde{\rho})$ and by Eq. (179) we have $\sigma < \sqrt{5}$. Requiring $|\hat{\mu} - F(\rho, \tilde{\rho})| \leq \epsilon$ and solving the right-hand sides leads to the sufficient condition $n_{\tilde{\rho}} \geq 160\epsilon^{-2} \ln(1/\delta)$. \blacksquare

Further reading

Shadow-fidelity estimation builds on the idea of extracting an incomplete description of a quantum state in order to subsequently estimate its properties. For such an incomplete description that correctly predicts the expectation of a set of observables Aaronson coined the term ‘‘shadow’’ in Ref. [19]. The broader framework for shadow estimation developed by Huang *et al.* [20,21] allows the sampling complexity of different measurement frames to be derived and is also not restricted to estimating fidelities. See also Pains and Kalev [73] for a parallel work analyzing the sampling complexity of estimating expectation values of observables from measurement frames that are generated using a group. Finally, we note that the linear cross-entropy benchmarking protocol [74] presented in Sec. III D similarly to SFE exploits a unitary 3-design as the measurement frame to achieve a sampling complexity scaling independently of the system size, as explicitly worked out by Helsen *et al.* [75].

III. QUANTUM PROCESSES

In the first part of this tutorial we present different approaches to certify quantum states. For the second part we now turn our attention to the certification of quantum processes, i.e., maps on quantum states.

As quantum technologies typically involve processing quantum states, the task of their certification is omnipresent. For example in quantum computing, processes of interest might be individual quantum gates, entire algorithms or a noise process that accounts for the deviation from the ideal functioning of a device.

Many of the methods developed for quantum states can be employed to derive analogous results for quantum processes. In principle, we can always arrive at a certificate for a quantum process by certifying its output states on a suitably large set of input states. Similarly, maximally entangling the input of a quantum process with ancillary quantum systems allows one to operationally prepare a

quantum state representing the quantum process via the so-called Choi-Jamiołkowski isomorphism.

After reviewing the mathematical formalism for describing quantum processes and discussing several measures of quality, we briefly discuss examples of translating methods for direct state certification to quantum processes.

As we see below, these approaches come with potentially severe drawbacks concerning the feasibility of the measurements. The characterization of a quantum process always involves the preparation of input states and measurements on the output of the process. In this task so-called state preparation and measurement (SPAM) errors can be a serious obstacle for a reliable characterization. This has motivated the development of quantum characterization and verification methods that are robust against such SPAM errors to quite some extent. One way to achieve this robustness are *self-consistent approaches* that aim at simultaneously characterizing quantum processes, the state preparation and the measurement [76–78]. These methods however require extensive effort in terms of the number of measurement settings, sampling complexity and classical postprocessing, and deliver far more information than required for certification.

An important class of certification methods in the context of digital quantum computing are *randomized benchmarking* protocols [66,79,80]. Randomized benchmarking protocols extract performance measures for quantum gates by implementing random gate sequences of different lengths and measuring the error that accumulates with the sequence length. By studying the error dependence in the sequence length randomized benchmarking protocols are robust against SPAM errors. We present two prototypical types of randomized benchmarking protocols targeting performance measures of a gate set and of individual gates together with the theoretical analysis in the simplest setup in Sec. III C.

Finally, in Sec. III D we turn our attention to a method that is used in order to certify the correct implementation of a quantum circuit in the context of demonstrating so-called quantum supremacy [we use the term “quantum (computational) supremacy” strictly in its established technical meaning [81]]: *cross-entropy benchmarking* [74].

A. Quantum processes and measures of quality

A *quantum process* should model possible operations taking quantum states to quantum states. Mathematically, a *quantum process* is, thus, a linear map taking density operators to density operators with suitable properties. Therefore, we start with introducing some notation related to linear maps between operator spaces.

In the following, let \mathcal{H}, \mathcal{K} be finite-dimensional Hilbert spaces. The vector space of linear maps from $L(\mathcal{H})$ to $L(\mathcal{K})$ is denoted by $\mathbb{L}(\mathcal{H}, \mathcal{K}) := L[L(\mathcal{H}), L(\mathcal{K})]$. We set $\mathbb{L}(\mathcal{H}) := \mathbb{L}(\mathcal{H}, \mathcal{H})$ and denote the identity by $\text{id}_{\mathcal{H}} :=$

$\mathbb{1}_{L(\mathcal{H})} \in \mathbb{L}(\mathcal{H})$. Often we just write id when it is clear from the context what \mathcal{H} is. A map $\Phi \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ is called *Hermicity preserving* if

$$\Phi[\text{Herm}(\mathcal{H})] \subset \text{Herm}(\mathcal{K}), \quad (186)$$

positive if

$$\Phi[\text{Pos}(\mathcal{H})] \subset \text{Pos}(\mathcal{K}), \quad (187)$$

and *trace preserving* if

$$\text{Tr}[\Phi(X)] = \text{Tr}[X] \quad (188)$$

for all $X \in L(\mathcal{H})$. Note that positive maps are also Hermicity preserving.

The map Φ is called *completely positive (CP)* if $\Phi \otimes \mathbb{1}_{L(\mathcal{H}'')}$ is positive for all Hilbert spaces \mathcal{H}' with identity map $\mathbb{1}_{L(\mathcal{H}'')} \in \mathbb{L}(\mathcal{H}'')$. The set of CP maps is denoted by $CP(\mathcal{H}, \mathcal{K}) \subset \mathbb{L}(\mathcal{H}, \mathcal{K})$ and forms a convex cone. We set $CP(\mathcal{H}) := CP(\mathcal{H}, \mathcal{H})$. A completely positive and trace preserving (CPT) map is also called a *quantum channel* or just *channel*. The subset of CPT maps is denoted by $CPT(\mathcal{H}, \mathcal{K}) \subset CP(\mathcal{H}, \mathcal{K})$ and forms a convex set. Again, we set $CPT(\mathcal{H}) := CPT(\mathcal{H}, \mathcal{H})$.

Lastly, a map $\Phi \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ is called *unital* if $\Phi(\mathbb{1}_{\mathcal{H}}) = \mathbb{1}_{\mathcal{K}}$. Note that Φ is trace preserving if and only if its adjoint (with respect to the Hilbert-Schmidt inner product) Φ^\dagger is unital.

So, essentially, quantum channels are maps that take density matrices to density matrices even when applied to a part of a larger system. Usual unitary dynamics is of the following form.

We use calligraphic letters to denote the adjoint representation $\mathcal{U} \in \mathbb{L}(\mathcal{H})$ of a unitary $U \in U(\mathcal{H})$ given by

$$\mathcal{U}(X) := UXU^\dagger. \quad (189)$$

These maps are quantum channels and are called *unitary (quantum) channels*.

Unitary channels are invertible and the inverses are again unitary channels.

1. The Choi-Jamiołkowski isomorphism

The Choi-Jamiołkowski isomorphism [82,83] provides a duality between CP maps and bipartite positive semidefinite operators and allows the identification of channels with certain states. It has many applications in quantum-information theory and related fields. In particular, it gives a practical criterion to check whether a given map is a quantum channel. Furthermore, it allows us to derive certification methods for quantum processes from the already presented methods for quantum states.

For any vector space V , recall that there is the canonical isomorphism

$$L(V) = V \otimes V^*, \quad (190)$$

where $V^* := L(V, \mathbb{C})$ is the dual space of V . Furthermore, if V is equipped with an inner product $\langle \cdot | \cdot \rangle$, we have the canonical isomorphism $v \mapsto (w \mapsto \langle v | w \rangle)$ identifying $V \stackrel{hc}{\cong} V^*$. For linear maps of linear maps $\mathbb{L}(\mathcal{H}, \mathcal{K})$ this simple isomorphism induces a couple of identifications with other vector spaces.

The *Choi-Jamiołkowski isomorphism*

$$\mathfrak{c} : \mathbb{L}(\mathcal{H}, \mathcal{K}) \rightarrow L(\mathcal{K} \otimes \mathcal{H}) \quad (191)$$

is one of these isomorphism of vector spaces given by the following sequence of simple identification:

$$\begin{aligned} \mathbb{L}(\mathcal{H}, \mathcal{K}) &= L(\mathcal{K}) \otimes L(\mathcal{H})^* = \mathcal{K} \otimes \mathcal{K}^* \otimes \mathcal{H}^* \otimes \mathcal{H} \\ &\cong \mathcal{K} \otimes \mathcal{H}^* \otimes \mathcal{K}^* \otimes \mathcal{H} = L(\mathcal{K} \otimes \mathcal{H}^*) \\ &\stackrel{hc}{\cong} L(\mathcal{K} \otimes \mathcal{H}), \end{aligned} \quad (192)$$

where the natural isomorphism, Eq. (190), is denoted by “=”, the isomorphism of changing the order of the vector spaces by “ \cong ”, and identification marked by “hc” makes use of the Hilbert space isomorphism $\mathcal{H} \cong \mathcal{H}^*$.

More explicitly, the Choi-Jamiołkowski isomorphism can be written in the following way. Let $(|i\rangle)_{i \in [\dim(\mathcal{H})]}$ be a basis of \mathcal{H} and

$$|\mathbb{1}\rangle = \sum_{i=1}^{\dim(\mathcal{H})} |i, i\rangle \in \mathcal{H} \otimes \mathcal{H} \quad (193)$$

the unnormalized maximally entangled state. The *Choi matrix* of $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ is given as

$$\mathfrak{c}(\mathcal{X}) = \mathcal{X} \otimes \text{id}(|\mathbb{1}\rangle\langle\mathbb{1}|). \quad (194)$$

This characterization of $\mathfrak{c}(\mathcal{X})$ implies

$$\text{Tr}[B\mathcal{X}(A)] = \text{Tr}[(B \otimes A^\top)\mathfrak{c}(\mathcal{X})] \quad (195)$$

for all $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$, $A \in L(\mathcal{H})$ and $B \in L(\mathcal{K})$, as can be seen by direct calculations with basis elements or tensor network diagrams.

Now we can connect the Choi-Jamiołkowski isomorphism to the properties of quantum channels.

Theorem 46 (CPT conditions): For any map $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ the following equivalences hold :

- (i) \mathcal{X} is trace preserving if and only if $\text{Tr}_{\mathcal{K}}[\mathfrak{c}(\mathcal{X})] = \mathbb{1}$.
- (ii) \mathcal{X} is Hermiticity preserving if and only if $\mathfrak{c}(\mathcal{X})$ is Hermitian.

- (iii) \mathcal{X} is completely positive if and only if $\mathfrak{c}(\mathcal{X})$ is positive semidefinite.

Proof. As an exercise or see, e.g., [84, Chapter 2.2]. ■

For completeness, we remark that another important consequence of the complete positivity of a map is the existence of so-called Kraus operators. This gives another item that could be added to Theorem 47: \mathcal{X} is a CP map if and only if there are (Kraus) operators $K_1, \dots, K_r \in L(\mathcal{H}, \mathcal{K})$, where $r = \text{rank}[\mathfrak{c}(\mathcal{X})]$ so that

$$\mathcal{X}(A) = \sum_{i=1}^r K_i A K_i^\dagger \quad (196)$$

for all $A \in L(\mathcal{H})$. Moreover, \mathcal{X} is a CPT map if and only if Eq. (196) holds with $\sum_{i=1}^r K_i^\dagger K_i = \mathbb{1}$.

In the context of quantum-information theory, another normalization convention for the Choi-Jamiołkowski isomorphism is useful. For $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ we set

$$\mathfrak{J}(\mathcal{X}) := \frac{1}{\dim(\mathcal{H})} \mathfrak{c}(\mathcal{X}) \quad (197)$$

with Choi matrix, Eq. (194). The theorem tells us that \mathcal{X} is a quantum channel if and only if $\mathfrak{J}(\mathcal{X})$ is a density matrix with the reduction to \mathcal{H} (obtained by tracing over \mathcal{K}) being a maximally mixed state. The so-called *Choi state* of a channel \mathcal{X} is

$$\mathfrak{J}(\mathcal{X}) = \mathcal{X} \otimes \text{id}_{\mathcal{H}}(\phi^+) \in \mathcal{S}(\mathcal{K} \otimes \mathcal{H}), \quad (198)$$

where

$$\phi^+ := \frac{1}{\dim(\mathcal{H})} |\mathbb{1}\rangle\langle\mathbb{1}| \in \mathcal{S}(\mathcal{H} \otimes \mathcal{H}) \quad (199)$$

is a *maximally entangled state*, i.e., has the strongest bipartite quantum correlations possible in a precise sense. In particular, the Choi state can be prepared by applying the channel to this state.

Note that not every bipartite state corresponds to a channel. Indeed, the Choi-Jamiołkowski isomorphism is an isomorphism of convex cones, $\mathfrak{c} : CP(\mathcal{H}, \mathcal{K}) \rightarrow Pos(\mathcal{K} \otimes \mathcal{H})$ but $CPT(\mathcal{H}, \mathcal{K})$ is mapped to a proper subset of $\mathcal{S}(\mathcal{K} \otimes \mathcal{H})$. The reason is that the trace-preservation constraint of channels corresponds to $\dim(\mathcal{H})^2$ many equalities whereas the trace constraint of states is just one equality.

An important quantum channel and frequent model for noise processes appearing in quantum technologies is the depolarizing channel. The (*quantum*) *depolarizing channel* $\mathcal{D}_p : L(\mathbb{C}^d) \rightarrow L(\mathbb{C}^d)$ with parameter $p \in [0, 1]$ is the linear map defined by

$$\mathcal{D}_p(X) := pX + (1-p)\text{Tr}[X]\frac{\mathbb{1}}{d}. \quad (200)$$

2. Inner products of superoperators and fidelity measures

The vector space of linear maps $\mathbb{L}(\mathcal{H}, \mathcal{K})$ is also equipped with a canonical inner product (the Hilbert-Schmidt inner product for superoperators) given by

$$\langle \mathcal{X}, \mathcal{Y} \rangle = \text{Tr}[\mathcal{X}^\dagger \mathcal{Y}] \quad (201)$$

for any $\mathcal{X}, \mathcal{Y} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$, where the trace can be calculated using an orthonormal basis $\{E_0, E_1, \dots, E_{d^2-1}\}$ of $L(\mathcal{H})$ as

$$\text{Tr}[\mathcal{X}] = \sum_{i=0}^{d^2-1} \langle E_i, \mathcal{X}(E_i) \rangle = \sum_{i=0}^{d^2-1} \text{Tr}[E_i^\dagger \mathcal{X}(E_i)]. \quad (202)$$

The Hilbert-Schmidt inner product on $\mathbb{L}(\mathcal{H}, \mathcal{K})$ coincides with the inner product of the corresponding Choi matrices, i.e., for any $\mathcal{X}, \mathcal{Y} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$

$$\langle \mathcal{X}, \mathcal{Y} \rangle = \langle \mathcal{C}(\mathcal{X}), \mathcal{C}(\mathcal{Y}) \rangle. \quad (203)$$

We now consider the case where \mathcal{Y} is a quantum channel and \mathcal{X} a unitary quantum channel. Then, as we see above, $\mathcal{J}(\mathcal{Y})$ and $\mathcal{J}(\mathcal{X})$ are quantum states (density matrices). Moreover, $\mathcal{J}(\mathcal{X})$ is a pure state. In this case, the above Hilbert-Schmidt inner product with the proper normalization is the fidelity measures induced by the state fidelity, Eq. (45), via the Choi-Jamiołkowski isomorphism, Eq. (194),

$$F_e(\mathcal{X}, \mathcal{Y}) := F[\mathcal{J}(\mathcal{X}), \mathcal{J}(\mathcal{Y})] = \frac{1}{\dim(\mathcal{H})^2} \langle \mathcal{X}, \mathcal{Y} \rangle; \quad (204)$$

it is referred to as the *entanglement (gate) fidelity*.

In the context of digital quantum computing, another very prominent fidelity measure for quantum processes is the so-called *average gate fidelity*. The *average gate fidelity* (AGF) between maps $\mathcal{X}, \mathcal{Y} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ is defined as

$$F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) := \int_{\mathbb{S}(\mathbb{C}^d)} \langle \mathcal{X}(|\psi\rangle\langle\psi|), \mathcal{Y}(|\psi\rangle\langle\psi|) \rangle d\mu_{\mathbb{S}(\mathbb{C}^d)}(\psi), \quad (205)$$

where the integral is taken according to the uniform Haar-invariant probability measure on state vectors of Sec. III 3. Note that the inner product here is the Hilbert-Schmidt inner product of $L(\mathcal{K})$ not $\mathbb{L}(\mathcal{H}, \mathcal{K})$. From the definition we see that the average gate fidelity $F_{\text{avg}}(\mathcal{X}, \mathcal{Y})$ is a measure of closeness of \mathcal{X} and \mathcal{Y} that compares the action of \mathcal{X} and \mathcal{Y} on pure input states on average. Intuitively, if \mathcal{X} and \mathcal{Y} deviate only in their action on a low-dimensional subspace of \mathcal{H} they can still have an average gate fidelity close to 1.

For any $\mathcal{X}, \mathcal{Y} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$

$$F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) = F_{\text{avg}}(\text{id}, \mathcal{X}^\dagger \circ \mathcal{Y}). \quad (206)$$

This motivates the definition $F_{\text{avg}}(\mathcal{X}) := F_{\text{avg}}(\text{id}, \mathcal{X})$ for $\mathcal{X} \in \mathbb{L}(\mathcal{H})$.

The average gate fidelity is intricately related to the Hilbert-Schmidt inner product on $\mathbb{L}(\mathcal{H}, \mathcal{K})$ [85,86] (see also Ref. [87]).

Proposition 47 (Inner product and F_{avg}): For $\mathcal{X}, \mathcal{Y} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ with $d = \dim \mathcal{H}$ it holds that

$$\langle \mathcal{X}, \mathcal{Y} \rangle = d(d+1)F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) - \langle \mathcal{X}(\mathbb{1}), \mathcal{Y}(\mathbb{1}) \rangle. \quad (207)$$

This proposition implies that the average gate fidelity is an inner product, i.e., a conjugate symmetric nondegenerate form that is linear in its second argument. For Hermiticity-preserving \mathcal{X} and \mathcal{Y} the average gate fidelity is real, $F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) \in \mathbb{R}$. Thus, on Hermiticity-preserving maps it is *symmetric*,

$$F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) = F_{\text{avg}}(\mathcal{Y}, \mathcal{X}). \quad (208)$$

Associate to the average gate fidelity is the *average error rate* or *average infidelity*,

$$r(\mathcal{X}, \mathcal{Y}) := 1 - F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) \quad (209)$$

that is also real valued for Hermiticity-preserving maps. We set $r(\mathcal{X}) := 1 - F_{\text{avg}}(\mathcal{X})$. For unital, completely positive \mathcal{X} , the average infidelity can be regarded as a distance to other quantum channels in the following sense.

Lemma 48 (Infidelity as distance measure): Let $\mathcal{X} \in CP(\mathcal{H}, \mathcal{K})$ be unital. For all $\mathcal{Y} \in CPT(\mathcal{H}, \mathcal{K})$ it holds that $r(\mathcal{X}, \mathcal{Y}) \geq 0$ and, $r(\mathcal{X}, \mathcal{Y}) = 0$ if and only if $\mathcal{X} = \mathcal{Y}$.

Proof. Using Proposition 48, we have $F_{\text{avg}}(\mathcal{Y}) = 1/[d(d+1)]\langle \text{id}, \mathcal{Y} \rangle + 1/(d+1)$. The overlap of the two CP maps can be bounded via the Cauchy-Schwarz inequality as $\langle \text{id}, \mathcal{Y} \rangle \leq \|\text{id}\|_F \|\mathcal{Y}\|_F$ with equality if and only if $\mathcal{Y} = \text{id}$. For $\mathcal{Y} \in CPT(\mathcal{H})$ it holds that $\|\mathcal{Y}\|_F^2 \leq d^2$ and $\|\text{id}\|_F^2 = d^2$. This can be seen, e.g., from the basis expansion, Eq. (202), by choosing a unit-rank basis and applying the Hölder inequality, Eq. (36). Therefore, $\langle \text{id}, \mathcal{Y} \rangle \leq d^2$. We conclude that $F_{\text{avg}}(\mathcal{Y}) \leq 1$ again with equality if and only if $\mathcal{Y} = \text{id}$, which implies the assertion. ■

We still have to prove Proposition 48.

Proof of Proposition 48. By the virtue of Eq. (206), which also holds for the inner products appearing in Eq.(207) it suffices to prove the statement for $\mathcal{X} = \text{id}$. Using Eq. (195) and denoting the transposition map as $T : L(\mathcal{H}) \rightarrow L(\mathcal{H})$,

$A \mapsto A^\top$, we can rewrite the average gate fidelity as

$$\begin{aligned}
F_{\text{avg}}(\text{id}, \mathcal{Y}) &= \int_{\mathbb{S}(\mathbb{C}^d)} \langle |\psi\rangle\langle\psi|, \mathcal{Y}(|\psi\rangle\langle\psi|) \rangle d\mu_{\mathbb{S}(\mathbb{C}^d)}(\psi) \\
&= \int_{\mathbb{S}^{d-1}} \text{Tr} [|\psi\rangle\langle\psi| \mathcal{Y}(|\psi\rangle\langle\psi|)] d\mu_{\mathbb{S}(\mathbb{C}^d)}(\psi) \\
&= \int_{\mathbb{S}(\mathbb{C}^d)} \text{Tr} [\text{id} \otimes T(|\psi\rangle\langle\psi|^{\otimes 2}) \mathcal{C}(\mathcal{Y})] d\mu_{\mathbb{S}(\mathbb{C}^d)}(\psi).
\end{aligned} \tag{210}$$

Due to linearity, we can recast this expression with the moment operator $K_{\mu_{\mathbb{S}(\mathbb{C}^d)}}^{(k)}$ of random states and use the expression we derive in Lemma 39. Then,

$$\begin{aligned}
F_{\text{avg}}(\text{id}, \mathcal{Y}) &= \text{Tr} \left[\text{id} \otimes T \left(K_{\mu_{\mathbb{S}(\mathbb{C}^d)}}^{(2)} \right) \mathcal{C}(\mathcal{Y}) \right] \\
&= \frac{2}{d(d+1)} \text{Tr} [\text{id} \otimes T(P_{\text{sym}^2}) \mathcal{C}(\mathcal{Y})] \\
&= \frac{1}{d(d+1)} \{ \text{Tr} [\mathbb{1} \mathcal{C}(\mathcal{Y})] + \text{Tr} [|\mathbb{1}\rangle\langle\mathbb{1}| \mathcal{C}(\mathcal{Y})] \},
\end{aligned} \tag{211}$$

where the last step follows from $P_{\text{sym}^2} = \frac{1}{2}(\mathbb{1} + \mathbb{F})$ with the swap operator \mathbb{F} from Eq. (6) and $\text{id} \otimes T(\mathbb{F}) = |\mathbb{1}\rangle\langle\mathbb{1}|$. Using Eq. (195) this time the other way around, we see that the first summand of Eq. (211) is $\text{Tr}[\mathbb{1} \mathcal{C}(\mathcal{Y})] = \text{Tr}[\mathbb{1} \otimes \mathbb{1} \mathcal{C}(\mathcal{Y})] = \text{Tr}[\mathcal{Y}(\mathbb{1})] = \langle \text{id}(\mathbb{1}), \mathcal{Y}(\mathbb{1}) \rangle$. From Eq. (194) it directly follows that $\mathcal{C}(\text{id}) = |\mathbb{1}\rangle\langle\mathbb{1}|$. Hence, the second term of Eq. (211) is $\text{Tr}[|\mathbb{1}\rangle\langle\mathbb{1}| \mathcal{C}(\mathcal{Y})] = \text{Tr}[\mathcal{C}(\text{id}) \mathcal{C}(\mathcal{Y})] = \langle \mathcal{C}(\text{id}), \mathcal{C}(\mathcal{Y}) \rangle = \langle \text{id}, \mathcal{Y} \rangle$. Plugging these two expressions into Eq. (211) and solving for $\langle \text{id}, \mathcal{Y} \rangle$ yields the assertion of the proposition. ■

If $\mathcal{X}^\dagger \mathcal{Y}$ trace-preserving, Eq. (207) simplifies to

$$\langle \mathcal{X}, \mathcal{Y} \rangle = d(d+1)F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) - d, \tag{212}$$

or, equivalently,

$$F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) = \frac{\langle \mathcal{X}, \mathcal{Y} \rangle + d}{d(d+1)}. \tag{213}$$

We conclude that for trace preserving and unital quantum channels the average gate fidelity and the Hilbert-Schmidt inner product are affinely related with a proportionality constant in $O(d^{-2})$. This is the same scaling as appearing for the entanglement fidelity in Eq. (204). More precisely, we find the affine relation between the two fidelities

$$F_{\text{avg}}(\mathcal{X}, \mathcal{Y}) = \frac{dF_e(\mathcal{X}, \mathcal{Y}) + 1}{d+1}, \tag{214}$$

still assuming $\mathcal{X}^\dagger \mathcal{Y}$ being trace preserving and one of \mathcal{X} and \mathcal{Y} being a unitary channel. For two unitary channels

$\mathcal{U}, \mathcal{V} \in \text{CPT}(\mathcal{H})$ with $U, V \in U(d)$ we can further simplify Eq. (213) to

$$F_{\text{avg}}(\mathcal{V}, \mathcal{U}) = \frac{|\text{Tr}[V^\dagger U]|^2 - d}{d(d+1)}. \tag{215}$$

For $V = \mathbb{1}$ this equality reflects that the average gate fidelity measures how close U is to $\mathbb{1}$ on average where the average is taken over its spectrum.

Furthermore, the identity, Eq. (207), also connects the average gate fidelity to the Frobenius norm. This, in turn, shows that the Frobenius norm is an average case error measure as well.

Lastly, beside the entanglement fidelity, the Hilbert-Schmidt inner product, the average gate fidelity, there is another affinely related measure of quality that is particularly convenient to work with in the analysis of randomized benchmarking: the effective depolarizing parameter. Here, we define the effective depolarizing parameter only for trace-preserving maps via its linear relation to the fidelity. If \mathcal{X} is not trace preserving one can more generally define it by explicitly first projecting on unital maps. Let $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ be trace preserving, its *effective depolarizing parameter* is

$$p(\mathcal{X}) := \frac{dF_{\text{avg}}(\mathcal{X}) - 1}{d-1}. \tag{216}$$

To justify its name let us have a look at the depolarizing channel \mathcal{D}_p , which is defined in Eq. (200) as the convex combination of $\mathcal{D}_1 = \text{id}$ and \mathcal{D}_0 . The average gate fidelity of these extremal channel can be quickly calculated to be $F_{\text{avg}}(\text{id}) = 1$ and $F_{\text{avg}}(\mathcal{D}_0) = 1/d$. Thus, $F_{\text{avg}}(\mathcal{D}_p) = p + (1-p)/d$. Plugging this into the definition of the effective depolarizing parameter, Eq. (216), yields

$$p(\mathcal{D}_p) = p. \tag{217}$$

Another affinely related measure that is often used in this context is the $\chi_{0,0}$ entry of the so-called χ -process matrix, see, e.g., Ref. [88] for further details.

3. The diamond norm

The distance measures on quantum channels we encounter so far can be regarded as average error measures. A more pessimistic, worst-case error measure is induced by the trace norm on operators, the so-called *diamond norm*. It measures the operational distinguishability of quantum channels. Hence, it plays an important role in the certification of quantum processes. Indeed, also error-correction thresholds require worst-case guarantees without additional assumption on the error model, see, e.g., the discussion Refs. [87,89]. At the same time, certification schemes that directly deliver certificate in diamond norm

are very resource intense and typically practically infeasible. For this reason, the connection of the diamond norm to the already introduced average error measures is the focus of this section.

We start with defining the $(1 \rightarrow 1)$ -norm on $\mathbb{L}(\mathcal{H}, \mathcal{K})$ to be the operator norm induced by the trace norm,

$$\|\mathcal{X}\|_{1 \rightarrow 1} := \sup_{\|A\|_1 \leq 1} \|\mathcal{X}(A)\|_1. \quad (218)$$

Note that if \mathcal{X} is Hermiticity preserving then the supremum is attained for a Hermitian operator since in that case $\mathcal{X}(A) = \frac{1}{2}[\mathcal{X}(A) + \mathcal{X}(A)^\dagger] = \mathcal{X}[\frac{1}{2}(A + A^\dagger)]$. Moreover, since the trace norm is a convex function, we have for any $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$

$$\|\mathcal{X}\|_{1 \rightarrow 1} = \sup_{|\psi\rangle, |\phi\rangle \in \mathbb{S}^{\dim(\mathcal{H})-1}} [|\langle \mathcal{X}(|\psi\rangle\langle\phi|) \rangle|]. \quad (219)$$

This means that the supremum is attained for rank-1 operators. For a Hermiticity preserving $\mathcal{X} \in \mathbb{L}(\mathcal{H})$, the supremum is furthermore attained at $|\psi\rangle = |\phi\rangle$. Density operators are normalized in trace norm. This implies that channels are normalized in $(1 \rightarrow 1)$ -norm, i.e.,

$$\|\mathcal{X}\|_{1 \rightarrow 1} = 1 \quad \forall \mathcal{X} \in CPT(\mathcal{H}, \mathcal{K}). \quad (220)$$

In order to distinguish quantum channels one can use ancillary systems. For this reason, we want to define a norm that has good stability properties for the maps acting on composite Hilbert spaces. This motivates the definition of the diamond norm as a so-called *completely boundedness (CB) completion* of the $(1 \rightarrow 1)$ -norm. We define *diamond norm* for $\mathcal{X} \in \mathbb{L}(\mathcal{H})$ by

$$\|\mathcal{X}\|_\diamond := \|\mathcal{X} \otimes \text{id}_{\mathcal{H}}\|_{1 \rightarrow 1}. \quad (221)$$

Note that the diamond norm inherits the above mentioned properties from the $(1 \rightarrow 1)$ -norm and preserves them even when a map is applied only to part of a composite Hilbert space. More precisely, the diamond norm has the following properties.

Theorem 49: (Complete boundedness and (sub)multiplicativity): For any $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$

$$\|\mathcal{X}\|_\diamond := \sup_{\mathcal{H}'} \|\mathcal{X} \otimes \text{id}_{\mathcal{H}'}\|_{1 \rightarrow 1}, \quad (222)$$

where the supremum is taken over all finite-dimensional Hilbert spaces \mathcal{H}' . Moreover,

$$\|\mathcal{X} \otimes \mathcal{Y}\|_\diamond = \|\mathcal{X}\|_\diamond \|\mathcal{Y}\|_\diamond, \quad (223)$$

$$\|\mathcal{X}\mathcal{Z}\|_\diamond \leq \|\mathcal{X}\|_\diamond \|\mathcal{Z}\|_\diamond \quad (224)$$

for all $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$, $\mathcal{Y} \in \mathbb{L}(\mathcal{H}', \mathcal{K}')$, and $\mathcal{Z} \in \mathbb{L}(\mathcal{H}', \mathcal{H})$.

Proof. For the proof we refer, e.g., to Ref. [84, Chapter 3.3] or recommend proving it as an exercise. ■

Theorem 50 tells us that the diamond norm precisely captures the maximum distinguishability of quantum channels $\mathcal{X}, \mathcal{Y} \in CPT(\mathcal{H}, \mathcal{K})$ in the following sense. One can prepare copies of a state $\rho \in \mathcal{S}(\mathcal{H} \otimes \mathcal{H}')$ and apply either \mathcal{X} or \mathcal{Y} to the parts on \mathcal{H} to obtain states on $\mathcal{K} \otimes \mathcal{H}'$. Then Proposition 12 tells us that $\frac{1}{2} \|\Phi \otimes \text{id}_{\mathcal{H}'}(\rho)\|_1$ is the distinguishability of the output states. Taking the supremum over all (pure) states ρ yields the distinguishability of \mathcal{X} and \mathcal{Y} , which is given by the *diamond distance* $\frac{1}{2} \|\mathcal{X} - \mathcal{Y}\|_\diamond$. In particular, the theorem tells us that optimal distinguishability can be obtained by choosing $\mathcal{H}' = \mathcal{H}$ in a similar sense as it can be detected when a map is not CP just using $\mathcal{H}' = \mathcal{H}$, cp. Theorem 47(iii).

Another way to distinguish quantum processes is to prepare their Choi states and distinguish them, as characterized by Proposition 12 via the trace norm. The following statements provide a relation of the two notions of distinguishability of quantum channels.

Proposition 50 (Diamond norm and trace norm): For any map $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$

$$\|\mathcal{J}(\mathcal{X})\|_1 \leq \|\mathcal{X}\|_\diamond \leq \dim(\mathcal{H}) \|\mathcal{J}(\mathcal{X})\|_1, \quad (225)$$

where \mathcal{J} denotes the Choi-Jamiołkowski isomorphism, Eq. (198).

The upper bound can be improved. For a Hermitian-preserving map $\mathcal{X} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ the improved bound implies [90, Corollary 2]

$$\|\mathcal{X}\|_\diamond \leq \dim(\mathcal{H}) \|\text{Tr}_2[|\mathcal{J}(\mathcal{X})\rangle]\|_\infty. \quad (226)$$

Proof of Proposition 51. We prove the proposition in terms of $\mathcal{C}(\mathcal{X}) = \dim(\mathcal{H}) \mathcal{J}(\mathcal{X})$. Denoting the Frobenius norm again by $\|\cdot\|_F$, it holds that

$$\|\mathcal{X}\|_\diamond = \sup_{\substack{A, B \in L(\mathcal{H}) \\ \|A\|_F = \|B\|_F = 1}} [|\langle (\mathbb{1} \otimes A) \mathcal{C}(\mathcal{X}) (\mathbb{1} \otimes B) \rangle|], \quad (227)$$

as can be seen from Eq. (219) and rearranging the contractions. Choosing $A = B = \mathbb{1}/\sqrt{\dim(\mathcal{H})}$ [corresponding to the maximally entangled state Eq. (199)] establishes the lower bound. The upper bound follows using Hölder's inequality, Eq. (36),

$$\begin{aligned} & \|(\mathbb{1} \otimes A) \mathcal{C}(\mathcal{X}) (\mathbb{1} \otimes B)\|_1 \\ & \leq \|\mathbb{1} \otimes A\|_{\text{op}} \|\mathcal{C}(\mathcal{X})\|_1 \|\mathbb{1} \otimes B\|_{\text{op}} \\ & = \|\mathbb{1}\|_{\text{op}} \|A\|_{\text{op}} \|\mathcal{C}(\mathcal{X})\|_1 \|\mathbb{1}\|_{\text{op}} \|B\|_{\text{op}} \\ & \leq \|A\|_F \|B\|_F \|\mathcal{C}(\mathcal{X})\|_1, \end{aligned} \quad (228)$$

and our normalization convention, Eq. (197). ■

It is not difficult to see that the bounds in Proposition 51 are tight, i.e., that there are $\mathcal{X}, \mathcal{Y} \in \mathbb{L}(\mathcal{H}, \mathcal{K})$ so that $\|\mathcal{J}(\mathcal{X})\|_1 = \|\mathcal{X}\|_\diamond$ and $\|\mathcal{X}\|_\diamond = \dim(\mathcal{H}) \|\mathcal{J}(\mathcal{X})\|_1$. These results tell us that distinguishing quantum channels via their Choi states is in general not optimal.

It is nonobvious how the diamond norm can actually be computed in practice. Watrous has shown that the diamond norm can be computed efficiently (in the dimension) via a semidefinite program [91]. However, for the highly relevant special case where the map is a difference of two unitary channels the computation is much simpler.

Proposition 51: (Diamond-norm distance of unitary channels): For any $U, V \in U(d)$ the diamond-norm distance of the corresponding unitary channels is

$$\frac{1}{2} \|\mathcal{U} - \mathcal{V}\|_\diamond = \sqrt{1 - \text{dist}(0, \text{conv}\{\lambda_i\}_{i \in [d]})^2}, \quad (229)$$

where λ_i are the eigenvalues of $U^\dagger V$, $\text{dist}(\cdot, \cdot)$ denotes the Euclidean distance and $\text{conv}(\cdot)$ the convex hull, both in the complex plane.

This proposition reflects that the diamond distance is a worst-case quantity, where the worst-case optimization is done over the spectrum of the “unitary difference” $U^\dagger V$. The geometric interpretation of this result is reviewed and visualized in Ref. [92].

In order to prove the proposition we write the matrices U and V as vectors. In general, (column) vectorization is a map $|\cdot\rangle : \mathbb{C}^{n_1 \times n_2} \rightarrow \mathbb{C}^{n_1 n_2}$ that stacks the columns of a matrix $A \in \mathbb{C}^{n_1 \times n_2}$ on top of each other. For all matrices A , B , and C with fitting dimensions it holds that

$$|ABC\rangle = C^\top \otimes A|B\rangle, \quad (230)$$

where $X \otimes Y \cong (X_{ij} Y)_{ij}$ (defined by a block matrix) denotes the Kronecker product of matrices X and Y .

Proof of Proposition 52. Starting with Eq. (219) and using the Choi-Jamiołkowski isomorphism, Eq. (195), and the vectorization rules for matrix products, Eq. (230), we can write the diamond norm of the channel difference as

$$\begin{aligned} \|\mathcal{U} - \mathcal{V}\|_\diamond &= \sup_{\substack{A \in L(\mathbb{C}^d) \\ \|A\|_2=1}} [\|(\mathbb{1} \otimes A)(|U\rangle\langle U| - |V\rangle\langle V|)(\mathbb{1} \otimes A)\|_1] \\ &= \sup_{\|A\|_2=1} \{ \| |AU\rangle\langle AU| - |AV\rangle\langle AV| \|_1 \} \\ &= \sup_{\|A\|_2=1} \{ \| |A\rangle\langle A| - |AU^\dagger V\rangle\langle AU^\dagger V| \|_1 \}. \end{aligned} \quad (231)$$

Using Eq. (47) relating the trace-norm difference of two trace-normalized, hermitian, unit-rank matrices to their

overlap yields

$$\begin{aligned} \frac{1}{2} \|\mathcal{U} - \mathcal{V}\|_\diamond &= \sup_{\|A\|_2=1} \left\{ \sqrt{1 - |\langle A|AU^\dagger V\rangle|^2} \right\} \\ &= \sup_{\|A\|_2=1} \left\{ \sqrt{1 - |\text{Tr}[A^2 U^\dagger V]|^2} \right\} \\ &= \sup_{\rho \in \mathcal{S}(\mathbb{C}^d)} \left\{ \sqrt{1 - |\text{Tr}[\rho U^\dagger V]|^2} \right\} \\ &= \sqrt{1 - \min_{\rho \in \mathcal{S}(\mathbb{C}^d)} |\text{Tr}[\rho U^\dagger V]|^2} \\ &= \sqrt{1 - \min_{\substack{p \in [0,1]^d \\ \sum_i p_i = 1}} \left| \sum_i p_i \lambda_i \right|^2} \\ &= \sqrt{1 - \text{dist}(0, \text{conv}\{\lambda_i\})}. \end{aligned} \quad (232)$$

■

Practical certification schemes for quantum processes will typically certify w.r.t. the Hilbert-Schmidt overlap, average gate fidelity or an equivalent quantity. In terms of the infidelity $r(\mathcal{X}) = 1 - F_{\text{avg}}(\mathcal{X})$, the diamond norm and the average gate fidelity are in general related by the following inequalities.

Proposition 52: (Infidelity and diamond norm [93, Proposition 9]): For any $\mathcal{X} \in \text{CPT}(\mathbb{C}^d)$ it holds that

$$\frac{d+1}{d} r(\mathcal{X}) \leq \frac{1}{2} \|\text{id} - \mathcal{X}\|_\diamond \leq \sqrt{d(d+1)r(\mathcal{X})}. \quad (233)$$

Proof. The proof combines Proposition 51 with the Fuchs-van de Graaf inequality, Eq. (46). Latter yields

$$\begin{aligned} 1 - F[\mathcal{J}(\text{id}), \mathcal{J}(\mathcal{X})] &\leq \frac{1}{2} \|\mathcal{J}(\text{id}) - \mathcal{J}(\mathcal{X})\|_1 \leq \sqrt{1 - F[\mathcal{J}(\text{id}), \mathcal{J}(\mathcal{X})]}, \end{aligned} \quad (234)$$

where we already drop a square root on the lower bound.

Since $\mathcal{J}(\text{id}) = (1/d)|\mathbb{1}\rangle\langle\mathbb{1}|$ is of unit rank and Hermitian, it holds that $F[\mathcal{J}(\text{id}), \mathcal{J}(\mathcal{X})] = \langle \mathcal{J}(\text{id}), \mathcal{J}(\mathcal{X}) \rangle = F_e(\text{id}, \mathcal{X})$. We can cast this in terms of the average gate fidelity via Eq. (214),

$$F[\mathcal{J}(\text{id}), \mathcal{J}(\mathcal{X})] = \frac{d+1}{d} F_{\text{avg}}(\mathcal{X}) - \frac{1}{d}. \quad (235)$$

Plugging Eq. (235) into Eq. (234) yields

$$\begin{aligned} \frac{d+1}{d} [1 - F_{\text{avg}}(\mathcal{X})] &\leq \frac{1}{2} \|\mathcal{J}(\text{id}) - \mathcal{J}(\mathcal{X})\|_1 \leq \sqrt{\frac{d+1}{d}} \sqrt{1 - F_{\text{avg}}(\mathcal{X})}. \end{aligned} \quad (236)$$

Finally, from Proposition 51 the proposition’s assertion follows. ■

Proposition 53 leaves us with an unsatisfactory state of affairs in two regards: first, the upper bound of the diamond norm introduces a dimensional factor $O(d)$. In the context of quantum computing, this leaves us with a potentially large factor scaling exponentially $O(2^n)$ with the number of qubits n . Second, the upper bound scales with the square root of the infidelity. For unitary quantum channels one can in fact tighten the lower bound to $\sqrt{r(\mathcal{X})}$ [87]. The lower bound for unitary quantum channels indicates that the square-root scaling is unavoidable in general. Practically, this means that to certify in diamond norm requires a certificate in infidelity that is orders of magnitude smaller. Particularly, for small system sizes this can be a key obstacle for the certification of the worst-case performance of quantum processes.

Fortunately, if a quantum process is highly incoherent, i.e., far away from being unitary, one can derive a linear scaling of the diamond-norm distance in the infidelity. The incoherence can be controlled by the so-called unitarity introduced by Wallman *et al.* [94]. For $\mathcal{X} \in \mathbb{L}(\mathcal{H})$ the *unitarity* is defined as

$$u(\mathcal{X}) = \frac{d}{d-1} F_{\text{avg}}(\mathcal{X}', \mathcal{X}'), \quad (237)$$

where $d = \dim \mathcal{H}$ and $\mathcal{X}' \in \mathbb{L}(\mathcal{H})$ is the defined by

$$\mathcal{X}'(A) = \mathcal{X}(A) - \text{Tr}[\mathcal{X}(A)]\mathbb{1}/\sqrt{d}. \quad (238)$$

One can straightforwardly check that $u(\mathcal{U}) = 1$ for every unitary channel \mathcal{U} . On the other hand, in Refs. [87,94] a lower bound on u in terms of the infidelity r is derived for trace-decreasing maps. For $\mathcal{X} \in \mathbb{L}(\mathcal{H})$ and $\text{Tr}[\mathcal{X}(\mathbb{1})] \leq \text{Tr}[\mathbb{1}]$ it holds that

$$u(\mathcal{X}) \geq u_{\min} = \left[1 - \frac{d}{d-1} r(\mathcal{X}) \right]^2. \quad (239)$$

Kueng *et al.* [87] established that quantum channels saturating this lower bound exhibit a linear scaling of the diamond-norm distance in terms of the infidelity.

Theorem 53: (Worst-case bound for incoherent channels [87, Theorem 3]): Let $\mathcal{X} \in \text{CPT}(\mathcal{H})$ be unital, $d = \dim(\mathcal{H})$. $\|\text{id} - \mathcal{X}\|_{\diamond} \in O[r(\mathcal{X})]$ if $u = u_{\min} + O[r^2(\mathcal{X})]$.

We leave it with this qualitative statement and refer to Ref. [87, Proposition 3] for a quantitative statement. See also Ref. [95].

B. Direct quantum-process certification

We see in Sec. II B, that quantum states can be certified with measurement strategies resembling the optimal

POVM P^+ for distinguishing quantum states of Proposition (12). By means of the Choi-Jamiołkowski isomorphism strategies for quantum states can be lifted to quantum processes: operationally, one prepares the Choi state, Eq. (194), by applying the process to a state that is maximally entangled with an ancillary system. Then one certifies the Choi state using a protocol for quantum states. The resulting certification protocols certifies with respect to the entanglement gate fidelity, Eq. (204), of the channels that coincides with the state fidelity of the Choi states.

References [96–98] use the direct state certification method of Sec. II B [24,25] in this way.

Moreover, for certain measurement strategies the protocol can be performed without using entanglement with ancillary systems. These, *prepare-and-measure versions* use an effective measurement strategy Ω of the form [96]

$$\Omega = \sum_i p_i N_i \otimes \rho_i^{\top}. \quad (240)$$

For this measurement strategy the expectation value in the Choi state is

$$\text{Tr}[\Omega \mathcal{J}(\tilde{\mathcal{U}})] = \sum_i p_i \text{Tr}[(N_i \otimes \rho_i^{\top}) \mathcal{J}(\tilde{\mathcal{U}})] \quad (241)$$

and can be recast, thanks to Eq. (195), as

$$\text{Tr}[(N_i \otimes \rho_i^{\top}) \mathcal{J}(\tilde{\mathcal{U}})] = \text{Tr}[N_i \tilde{\mathcal{U}}(\rho_i)]. \quad (242)$$

While the dichotomic POVM defined by $N_i \otimes \rho_i^{\top}$ for each i originally acts on the Choi state $\mathcal{J}(\tilde{\mathcal{U}})$, the form of Eq. (242) suggests a simpler, straight-forward experimental implementation: of the dichotomic POVM: one prepares the state ρ_i , applies the channel \mathcal{U} under scrutiny, and measures the dichotomic POVM given by N_i on the state $\tilde{\mathcal{U}}(\rho_i)$. Thus, effective measurement strategies of the form [96] can indeed be implemented by simple prepare-and-measure schemes.

For Clifford unitaries this method yields a simple direct certification test. The Choi state of a Clifford unitary channel is a stabilizer state and can hence be verified with the methods of Ref. [24] discussed in Sec. II F 1. The following proposition gives a theoretical guarantee for this protocol. It can be derived as a corollary of the results of Sec. II F 1.

Proposition 54: (Direct certification of Clifford operations, [96, Proposition 3]): Let \mathcal{C} be an n -qubit Clifford operation. We consider the state certification of Protocol 17 applied to its Choi state $\mathcal{J}(\mathcal{C})$, which is a stabilizer state. This yields an ϵ -certification test of $\mathcal{J}(\mathcal{C})$ w.r.t. infidelity

from $n_{\bar{\rho}}$ independent such state preparations for

$$n_{\bar{\rho}} \geq 2 \frac{\ln(1/\delta)}{\epsilon} \quad (243)$$

with confidence $1 - \delta$. Moreover, the target $\mathcal{J}(\mathcal{C})$ is accepted with probability 1.

This test corresponds to a similar certification test of \mathcal{C} w.r.t. entanglement gate infidelity $1 - F_e$ and can be implemented as a prepare-and-measure scheme via Eq. (242).

Further reading

The three works of Refs. [96–98] all follow the presented certification strategy based on direct state certification. Moreover, they discuss several additional aspects: Liu *et al.* [96] study non-trace-preserving processes and measurements, Zhu and Zhang [97] analyze the general multi-qudit case and strategies based on projective 2-designs, and Zeng *et al.* [98] discuss entanglement-property detection.

Similar to direct state certification also fidelity estimation protocols can be lifted to quantum processes. To this end, one applies the state fidelity estimation to the output of the process applied to randomly chosen input states. The original DFE proposal by Flammia and Liu [43] already includes the application to quantum channels by sampling from the eigenstates of multiqubit Pauli operators as the input states. Furthermore, simplifications arising for Clifford gates are discussed. See also the parallel work by da Silva *et al.* [50]. A strategy to estimate the average gate fidelity by inputting states drawn at random from complex projective 2-designs was studied by Bendersky *et al.* [99]. Reich *et al.* [100] determined the minimal number of required input states for the fidelity estimation of quantum processes. See also the related work by Hofmann [101]. Reich *et al.* also provide a quantitative comparative overview over all the before-mentioned approaches in Ref. [102].

C. Randomized benchmarking

The schemes presented in the previous section fail in the presence of sizeable SPAM errors. In the context of digital quantum computing, this sensibility to SPAM errors is dramatically reduced by so-called *randomized benchmarking (RB)* protocols [66,79,80,103,104]. These protocols can extract certain quantitative measures of a quantum process associated to a *quantum-gate set*. The process can be, for example, a certain gate, an error channel or an error map associated to the deviation of a quantum-gate set from its ideal implementation. While still concerned with the physical layer of a quantum device, randomized benchmarking protocols already make explicit use of a gate layer, the abstraction at the heart of digital quantum computing.

Randomized benchmarking comprises a large zoo of different protocols. Therefore, we begin with a fairly general

description. The principle idea to achieve the SPAM-(error) robustness is the following: after preparing an input state, one applies the quantum process under scrutiny multiple times in sequences of different length before performing a measurement. Thereby, the effect of the process on the measurement is attenuated with increasing sequences length. At the same time errors in the state preparation and measurements enter the measured quantities only linearly and are independent of the sequence length. In this way, fitting the attained signals for different sequence lengths with functions depending on the length reveals properties of the quantum process disentangled from the SPAM errors.

A prototypical RB protocol implements this rough idea for a digital quantum computer as follows. Let $\mathbf{G} \subset U(d)$ be a subgroup of unitary operations and $\phi : \mathbf{G} \rightarrow \mathbb{L}(\mathbb{C}^d)$ be their implementation on a quantum computer. In simple RB protocols $\phi(g)$ just models the faulty implementation of \mathcal{G} on the actual device. More generally, the targeted implementation of the protocol can also include, e.g., a nonuniform sampling over the group or the implementation of another fixed gate after \mathcal{G} . Also in these cases ϕ is the faulty version of the targeted implementation.

Note that the assumption of the existence of such a map ϕ already encodes assumptions on the quantum device and its noise process: The map ϕ might model the compilation into elementary gates, effects and imperfections of the physical control and noise. All these steps are not allowed to depend on the gate sequence the gate is part of, the overall time that evolves during the protocol, or other external variables.

With these ingredients we can state a prototypical RB protocol, see Fig. 4 for an illustration.

Protocol 55 (Prototypical RB): Let $\mathbf{G} \subset U(d)$ be a subgroup, $\rho \in \mathcal{S}(\mathbb{C}^d)$ an initial state, and $\mathbf{M} = \{M, \mathbb{1} - M\} \subset \text{Pos}(\mathbb{C}^d)$ a measurement. Furthermore, let $\mathcal{M} \subset \mathbb{N}$ be a set of sequence lengths.

For every sequence length $m \in \mathcal{M}$, we do the following estimation procedure multiple times.

Draw a sequence $g = (g_1, \dots, g_m)$ of m group elements chosen i.i.d. uniformly at random. For the sequence calculate the inverse elements $g_{\text{inv}} = g_1^{-1} g_2^{-1} \dots g_m^{-1}$.

For each sequence perform the following experiment:

- (i) Prepare ρ .
- (ii) Apply $S_g = \phi(g_{\text{inv}})\phi(g_m) \dots \phi(g_2)\phi(g_1)$, i.e., the sequence of implementations of g followed by the implementation of g_{inv} , to ρ .
- (iii) Perform the measurement \mathbf{M} .

Multiple repetitions of the experiment yield an estimator \hat{p}_g for the probabilities

$$p_g(m) = \text{Tr}[MS_g\rho]. \quad (244)$$

Data collection phase

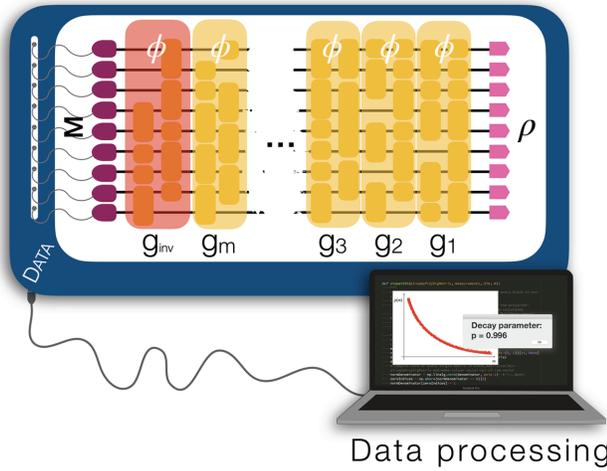


FIG. 4. Illustration of a prototypical RB protocol. After the preparation of an initial state, one applies a random sequence of unitaries $g = (g_1, \dots, g_m)$ succeeded by an inversion gate and final measurement of M . This experiment is repeated for different sequences and different sequence lengths m . In the classical postprocessing, the decay parameter of resulting empirical estimates for different sequence lengths m are extracted and reported as the RB parameters.

Repeating these steps for different random sequences, we can calculate an estimator $\hat{p}(m)$ for

$$p(m) = \mathbb{E}_{g_1} \mathbb{E}_{g_2} \dots \mathbb{E}_{g_m} P_{(g_1, g_2, \dots, g_m)}(m). \quad (245)$$

Postprocessing: extract the decay parameters of the data $M \rightarrow [0, 1]$, $m \mapsto \hat{p}(m)$ and report as the RB parameters.

More generally, RB protocols might go beyond Protocol 56 in various ways: for example, by calculating the inverse of a sequence only up to specific gates, using a different measure than the uniform measure for drawing the group elements of the sequence, or performing a measurement POVM with multiple outputs or measurements adapted to the sequence. In addition, the postprocessing might combine different RB data series in order to get simpler decay signatures.

The first step in the theoretical analysis of RB protocols is to establish the fitting model of the RB data $p(m)$. Ideally, $p(m)$ is well approximated by a single exponential decay. Subsequently, the RB decay parameters can in certain settings be connected to the average gate fidelity of a noise process effecting the implementation map, as we now discuss.

The data model of most RB protocols can be understood as estimating the m -fold self-convolution of the implementation map [105]. More precisely, for $\phi, \psi : \mathbf{G} \rightarrow \mathbb{L}(\mathbb{C}^d)$ we can define a convolution operation as

$$\phi * \psi(g) = \mathbb{E}_{\tilde{g}} \phi(g\tilde{g}^{-1})\psi(\tilde{g}). \quad (246)$$

Note that this definition naturally generalizes, e.g., the discrete circular convolution on vectors in \mathbb{C}^n , which can be seen as an operation on functions on the finite group $(\mathbb{Z}_n, +) \rightarrow \mathbb{C}$. With the convolution, Eq. (246), we can rewrite the averages of the RB sequences as

$$\begin{aligned} \mathbb{E}_g S_g &= \mathbb{E}_{g_1, g_2, \dots, g_m} \phi(g_1^{-1} g_2^{-1} \dots g_m^{-1}) \phi(g_m) \dots \phi(g_2) \phi(g_1) \\ &= \mathbb{E}_{h_1, h_2, \dots, h_m} \phi(h_m^{-1}) \phi(h_m h_{m-1}^{-1}) \dots \phi(h_2 h_1^{-1}) \phi(h_1) \\ &= \phi^{*(m+1)}(\text{id}), \end{aligned} \quad (247)$$

where the replacements $h_1 = g_1$ and $h_j = g_j h_{j-1}$ for $j \in \{2, \dots, m\}$ have been made the second equality, id denotes the identity element of \mathbf{G} and ϕ^{*k} denotes the k -fold convolution of ϕ with itself. In expectation the RB data $p(m)$ is thus a contraction defined by M and ρ of the $(m+1)$ -fold self-convolution of ϕ evaluated at the identity element.

In the simplest instance of an RB protocol one can directly calculate this expression: namely, when \mathbf{G} is a unitary 2-design, the targeted implementation is simply the action of \mathbf{G} as quantum gates, and the noise in ϕ can be modeled by a single gate-independent quantum channel $\Lambda \in CPT(\mathbb{C}^d)$. Denoting by \mathcal{G} the (adjoint) action of g as the unitary channel $X \mapsto \mathcal{G}(X) = gXg^\dagger$, we have the noise model

$$\phi(g) = \Lambda \circ \mathcal{G}. \quad (248)$$

With this ansatz for ϕ we can calculate that

$$\mathbb{E}_{g \in \mathbf{G}^m} S_g = \phi^{*(m+1)}(\text{id}) = \Lambda[\mathbb{E}_{g \in \mathbf{G}} \mathcal{G}^\dagger \Lambda \mathcal{G}]^m. \quad (249)$$

The operator $tw_\mu : \mathbb{L}(\mathbb{C}^d) \rightarrow \mathbb{L}(\mathbb{C}^d)$, $\mathcal{X} \mapsto \mathbb{E}_{U \sim \mu} [U \mathcal{X} U^\dagger]$ appearing in Eq. (249) is the so-called (*channel*) *twirling map* and appears in different contexts in quantum information. If we write out the twirling map with the individual unitaries it reads

$$tw_\mu(\mathcal{X}) = (\rho \mapsto \mathbb{E}_{U \sim \mu} \{U \mathcal{X} [U^\dagger(\rho) U] U^\dagger\}). \quad (250)$$

It becomes apparent that tw_μ is related to second moment operator $\mathcal{M}_\mu^{(2)}$, Eq. (137), by simple vector-space isomorphisms. Recall that for a unitary 2-design μ Proposition 37 gives us an explicit description of $\mathcal{M}_\mu^{(2)}$. We can simply track the isomorphism to derive the following convenient expression.

Theorem 56 (Twirling of channels [79,86]): Let $\mathcal{X} \in \mathbb{L}(\mathbb{C}^d)$ be trace preserving and μ be a unitary 2-design. Then

$$tw_\mu(\mathcal{X}) = \mathcal{D}_{p(\mathcal{X})}, \quad (251)$$

where \mathcal{D}_p is the depolarizing channel, Eq. (200), and $p(\mathcal{X})$ is the effective depolarizing parameter defined in Eq. (216).

Proof. First we note that any map $\mathcal{X} \in \mathbb{L}(\mathbb{C}^d)$ is uniquely determined by $(\mathcal{X} \otimes \text{id})(\mathbb{F})$, which is a similar construction as the Choi-Jamiołkowski isomorphism. This isomorphism is given by $\text{Tr}_{2,3}[(\mathcal{X} \otimes \text{id})(\mathbb{F}) \otimes A] = \mathcal{X}(A)$ but its explicit form is not needed. Hence, we can make the isomorphisms between the twirling map tw_μ and the second-moment operator $\mathcal{M}_\mu^{(2)}$ from Eq. (137) explicit by writing

$$\begin{aligned} & [tw_\mu(\mathcal{X}) \otimes \text{id}](\mathbb{F}) \\ &= \mathbb{E}_{U \sim \mu} \{ (U \otimes \mathbb{1}) \mathcal{X} \otimes \text{id} [(U^\dagger \otimes \mathbb{1}) \mathbb{F} (U \otimes \mathbb{1})] (U^\dagger \otimes \mathbb{1}) \} \\ &= \mathbb{E}_{U \sim \mu} \{ (U \otimes \mathbb{1}) \mathcal{X} \otimes \text{id} [(\mathbb{1} \otimes U) \mathbb{F} (\mathbb{1} \otimes U^\dagger)] (U^\dagger \otimes \mathbb{1}) \} \\ &= \mathbb{E}_{U \sim \mu} [(U \otimes U) \mathcal{X} \otimes \text{id}(\mathbb{F}) (U^\dagger \otimes U^\dagger)] \\ &= \mathcal{M}_\mu^{(2)}[\mathcal{X} \otimes \text{id}(\mathbb{F})]. \end{aligned} \quad (252)$$

For μ a unitary 2-design, $\mathcal{M}_\mu^{(2)}$ takes the value of the moment operator of the Haar measure. Schur-Weyl duality, Theorem 35, tells us that

$$\mathcal{M}_\mu^{(2)}[\mathcal{X} \otimes \text{id}(\mathbb{F})] \in \text{span}\{\mathbb{1}, \mathbb{F}\}. \quad (253)$$

Observing that $\mathcal{D}_0 \otimes \text{id}(\mathbb{F}) = \mathbb{1}/d$ and trivially $\mathcal{D}_1 \otimes \text{id}(\mathbb{F}) = \mathbb{F}$, we conclude that

$$tw_\mu(\mathcal{X}) \in \text{span}\{\mathcal{D}_0, \mathcal{D}_1\}. \quad (254)$$

Furthermore, one quickly checks that if \mathcal{X} is trace preserving so is $tw_\mu(\mathcal{X})$. Hence, $tw_\mu(\mathcal{X})$ is an affine combination of \mathcal{D}_0 and \mathcal{D}_1 . Thus, $tw_\mu(\mathcal{X}) = \mathcal{D}_p$ holds for some $p \in \mathbb{C}$ and it remains to determine p . One way forward is a straight-forward calculation using the expressions for the coefficients provided by Proposition 38. A shortcut is to calculate the effective depolarization of both sides. Due to the unitary invariance of $\mu_{\mathbb{S}(\mathbb{C}^d)}$, it follows from Eq. (205) that $F_{\text{avg}}(\mathcal{X}) = F_{\text{avg}}[tw_\mu(\mathcal{X})]$ and correspondingly for the affinely related effective depolarization parameter $p(\mathcal{X}) = p[tw_\mu(\mathcal{X})]$. Combined with $p(\mathcal{D}_p) = p$, Eq. (217), yields the theorem's assertion. \blacksquare

Theorem 57 allows us to explicitly calculate the RB data model from Eq. (249). To this end, a short calculation reveals that $\mathcal{D}_p^m = \mathcal{D}_{p^m}$. With this we find the RB data model to be

$$\begin{aligned} p(m) &= \text{Tr}[\tilde{M} \Lambda \mathcal{D}_{p(\Lambda)^m}(\tilde{\rho})] \\ &= p(\Lambda)^m \text{Tr}[\tilde{M} \Lambda(\tilde{\rho})] + [1 - p(\Lambda)^m] \text{Tr}[\tilde{M} \Lambda(\mathbb{1}/d)] \\ &= p(\Lambda)^m \text{Tr}[\tilde{M} \Lambda(\tilde{\rho} - \mathbb{1}/d)] + \text{Tr}[\tilde{M} \Lambda(\mathbb{1}/d)], \end{aligned} \quad (255)$$

with \tilde{M} and $\tilde{\rho}$ denoting the potentially faulty implementation of the measurement M and initial state ρ .

If we define the so-called *SPAM constants*

$$A := \text{Tr}[\tilde{E} \Lambda(\tilde{\rho} - \mathbb{1}/d)] \quad \text{and} \quad B := \text{Tr}[\tilde{E} \Lambda(\mathbb{1}/d)], \quad (256)$$

Eq. (255) yields the simple RB fitting model

$$p(m) = A p^m + B. \quad (257)$$

Thus, fitting a single exponential decay to the estimator $\hat{p}(m)$ yields estimates \hat{p} , \hat{A} and \hat{B} for the model parameters p , A , and B . In particular, the estimated RB decay parameter \hat{p} is an estimator for the effective depolarizing parameter $p(\Lambda)$ of the error channel Λ . Recall that the effective depolarizing parameter is affinely related to the average gate fidelity, Eq. (205) via Eq. (216). From the RB decay parameter, we thus equivalently obtain an estimate for the average gate fidelity of the noise channel Λ as

$$\hat{F}_{\text{avg}} = \left(1 - \frac{1}{d}\right) \hat{p} + \frac{1}{d}. \quad (258)$$

Note that the resulting estimate of Eq. (205) is robust against SPAM errors, which only enter the SPAM constants A and B .

Deriving rigorous performance guarantees for the estimator RB estimator \hat{p} is involved: it requires the analysis of confidence region of the estimator $\hat{p}_g(m)$ of Eq. (244) that is a random variable of the quantum-measurement statistics and $\hat{p}(m)$ obtained by the subsampling of the sequences g . Furthermore, the error of these estimators for each m enters the errors of the fidelity estimator via the exponential fitting procedure. This step depends on the choice of algorithm and the estimated sequence lengths.

Using the fact that $\hat{p}(m)$ is the mean estimator of a bounded random variable, one can use Hoeffding's inequality, Theorem 8, to derive confidence intervals for an overall sampling complexity that is independent of the number of qubits in the regime of high fidelity. Such bounds however are prohibitively large for practical implementations. A refined analysis by Wallman and Flammia [93] derived tighter bounds for short sequences and small number of qubits. However, bounds that are practical and scalable in the number of qubits require a careful analysis of the variance of the estimator $\hat{p}_g(m)$ over the choice of the random sequences. For \mathbf{G} being the Clifford group, Helsen *et al.* [106] work out explicit variance bounds for the estimator $\hat{p}_g(m)$ and derive sampling complexities for $\hat{p}(m)$ that are practical, independent of the number of qubits and scale favorable with the sequence length. To this end, they employed a refined representation theoretical analysis of the commutant of the fourth-order diagonal action of the Clifford group [61,107] in order to calculate the corresponding moment operator; an endeavour that is complicated by the fact that the Clifford group itself is not a unitary 4-design.

A rigorous analysis of a simplified fitting procedure was derived in Ref. [108]. Therein (again using trivial bounds on the variance) the authors show that a ratio estimator for the infidelity $r = 1 - p$ that employs the estimates of $p(m)$ for two different sequence length has multiplicative error using an efficient number of samples again in the regime of high fidelity.

All of these performance guarantees indicate that in principle RB protocols can be efficiently scalable in the number of qubits. To ensure also an efficient classical pre-processing of the prototypical RB protocol it is important to have an efficiently tractable group structure so that the inverse of the gate sequence can be computed.

For the important example of the Clifford group, the Gottesman-Knill theorem, see, e.g., [58], allows computation of the inverse of a sequence $g_m \cdots g_2 g_1$ in polynomial time (with respect to the number of qubits). Furthermore, since the Clifford group is a unitary 3-design [59,60], it meets the requirement of Theorem 57. For this reason the presented analysis applies to the Clifford group under the assumption of gate-independent noise.

It is natural to ask of additional examples of groups that constitute a unitary 2-design and are covered by the presented analysis without modifications. But it was established that these two requirements are already surprisingly restrictive. A complete classification of so-called 2-groups (2-design groups) is summarized in Ref. [109]. In fact, if one requires a family of 2-groups that can be constructed for an arbitrary number of qubits, one is left with subgroups of the Clifford group or $SU(d)$ itself as the only examples [109–111].

We provide more details how the analysis of the prototypical RB protocol can be generalized in the further-reading paragraph at the end of the section. Now, we want to discuss another variant of RB that is particularly important as tool for certifying quantum gates.

Interleaved randomized benchmarking

The prototypical RB protocol estimates the effective depolarizing parameter or the average gate fidelity of the average error channel of a gate *set*. In contrast, *interleaved RB* protocols [112] allow one to extract the effective depolarizing parameter of *individual* gates from a group with respect to their ideal implementation provided the noise is sufficiently incoherent.

In an interleaved RB protocol one performs in addition to the standard RB protocol a modified version, where the random sequences are interleaved with the specific target gate. The second experiment yields estimates for the effective depolarization parameter of the error channel associated to the group concatenated with the error channel of the individual target gate. Under certain assumptions the effective depolarization parameter of the implementation of the

target gate can be estimated from the decay parameters of both RB protocols.

Protocol 57 (Interleaved RB): For $\mathbf{G} \subset U(d)$ and a target gate $g_T \in \mathbf{G}$

- (1) follow Protocol 56,
- (2) follow Protocol 56 but modify the sequences to be

$$g = (g_1, g_T, g_2, g_T, g_3, \dots, g_T, g_m), \quad (259)$$

where g_T is the target gate and $g_i \in \mathbf{G}$ for $i \in [m]$ are drawn uniformly at random. The inverse g_{inv} is also calculated with respect to the modified sequence g .

The output of the protocol are the decay parameters of both experiments.

For the analysis we again consider a “mostly” gate-independent noise model and assume that \mathbf{G} is a unitary 2-design. In the noise model we assume that the same noise channel $\Lambda \in CPT(\mathcal{H})$ follows the ideal implementation of all gates but the target gate, i.e.,

$$\phi(g) = \Lambda \circ \mathcal{G} \quad (260)$$

for all $g \in \mathbf{G} \setminus \{g_T\}$.

The first step of the protocol is the unmodified RB protocol. If we neglect that ϕ deviates from the form, Eq. (260), on g_T , we can apply the analysis of the previous section for gate-independent noise and conclude that the protocol outputs and estimator for the effective depolarizing constant $p(\Lambda)$. For example, for a large group it is plausible to neglect the contribution of the noise associated to the g_T gate to the group average.

It remains to analyze the second protocol. In analogy to Eq. (246) we can in general rewrite

$$\begin{aligned} \mathbb{E}_{g_1, \dots, g_m} S_g &= \mathbb{E}_{g_1, \dots, g_m} \phi(g_1^{-1} g_T^{-1} g_2^{-1} g_T^{-1} \dots g_m^{-1}) \\ &\quad \times \phi(g_m) \phi(g_T) \dots \phi(g_2) \phi(g_T) \phi(g_1) \\ &= \mathbb{E}_{g_1, \dots, g_m} \phi(g_m^{-1}) \dots \\ &\quad \times \phi(g_3 g_2^{-1} g_T^{-1}) \phi(g_T) \phi(g_2 g_1^{-1} g_T^{-1}) \phi(g_T) \phi(g_1), \end{aligned}$$

by substituting g_i with $g_i g_{i-1}^{-1} g_T^{-1}$ for all $i > 1$.

Inserting the noise model, Eq. (260), yields

$$\mathbb{E}_{g_1, \dots, g_m} S_g = \Lambda \left[\mathbb{E}_{g \in \mathbf{G}} \mathcal{G}^\dagger \mathcal{G}_T^\dagger \phi(g_T) \Lambda \mathcal{G} \right]^m. \quad (261)$$

This is the same expression as Eq. (249) with Λ replaced by $\mathcal{G}_T^\dagger \phi(g_T) \Lambda$. Hence, applying the same arguments as in the analysis of the standard RB protocol for unitary 2-designs yields a single-exponential fitting model

with decay parameter estimating the effective depolarizing parameter $p[\mathcal{G}_T^\dagger\phi(g_T)\Lambda]$. The second part of the interleaved RB protocol, thus, yields an estimate of the effective depolarizing parameter or equivalently, via Eq. (258), of the fidelity of the error map $\mathcal{G}_T^\dagger\phi(g_T)$ of the target gate \mathcal{G}_T concatenated with the error channel Λ .

From $p(\Lambda)$ and $p[\mathcal{G}_T^\dagger\phi(g_T)]$ it is indeed possible to infer $p[\mathcal{G}_T^\dagger\phi(g_T)]$. In meaningful practical regimes this however requires additional control the unitarity of Λ [88]: for sequences of unitary channels the infidelity of their composition can scale quadratically in the sequence length in leading order. In contrast, highly nonunitary channels will feature a close to linear scaling in the sequence length. Thus, using the unitary one can derive bounds for fidelity measures of composite channels that exploit the linear scaling. We simply state the required bound without proof for interleaved RB.

Theorem 58 (Composite channel bound [88]): For any two quantum channels \mathcal{X}, \mathcal{Y} it holds that

$$\left| p(\mathcal{X}) - \frac{p(\mathcal{X}\mathcal{Y})p(\mathcal{Y})}{u(\mathcal{Y})} \right| \leq \sqrt{1 - \frac{p(\mathcal{Y})^2}{u(\mathcal{Y})}} \sqrt{1 - \frac{p(\mathcal{X})^2}{u(\mathcal{Y})}}. \quad (262)$$

With an estimate for the unitarity $\hat{u}(\Lambda)$, Theorem 59 allows estimation of the effective depolarizing constant and thus the average gate fidelity of the target gate by

$$\hat{F}_{\text{avg}}[\phi(g_T), \mathcal{G}_T] = \frac{d-1}{d} \frac{\hat{p}[\mathcal{G}_T^\dagger\phi(g_T)]\hat{p}(\Lambda)}{\hat{u}^\Lambda} + \frac{1}{d} \quad (263)$$

up to a systematic error that is given by evaluating the right-hand side of Eq. (262). The systematic error is small in the regime where $u(\Lambda) \approx p(\Lambda)^2$, which is the case if Λ is decoherent. The unitarity of Λ can be estimated using variants of the RB protocol itself developed in Refs. [94,113].

Alternatively, one can just assume that the error is sufficiently incoherent, i.e., that $|1 - p(\Lambda)^2/u(\Lambda)| \leq \epsilon$. Conditioned on this external belief, one obtains the simpler estimator

$$\hat{F}_{\text{avg}}[\phi(g_T), \mathcal{G}_T] = \frac{d-1}{d} \frac{\hat{p}[\mathcal{G}_T^\dagger\phi(g_T)]}{\hat{p}(\Lambda)} + \frac{1}{d} \quad (264)$$

that comes with a systematic error that is controlled in ϵ . Thereby, interleaved RB can be used to arrive at average-performance certificates of individual quantum gates.

We have already seen that for interleaved RB controlling the unitarity is helpful in deriving tighter error bounds. In addition, estimating the unitarity can also yield relevant worst-case performance bounds in terms of the average gate fidelities using Theorem 54.

Further reading

Randomized benchmarking was originally developed in a series of work focusing on the unitary group and Clifford gates [66,79,80,103,104].

The early analyses used the gate-independent noise model, Eq. (248), which we also assume here. In many applications this is however a questionable assumption. After first perturbative approaches to derive the RB signal model under gate-dependent noise by Magesan *et al.* [104,114] and Proctor *et al.* [115], Wallman rigorously derived the fitting model for unitary 2-designs in Ref. [116].

Using the elegant description of the RB data as the m -fold convolution of the implementation map, recently proposed by Merkel *et al.* [105], one can abstractly understand the result as follows: as the standard discrete circular convolution, the convolution operator of maps on a group can be turned into a (matrix) multiplication using a Fourier transform. This abstract Fourier transform for functions on the group is defined to be a function on the irreducible representations of the group. In the case of RB, this function is matrix valued, and we observe matrix powers of the Fourier transforms for every irreducible representation superimposed by a linear map. For every irreducible representation, for sufficiently large m , the matrix powers are proportional to the m th power of the largest eigenvalue of the matrix-valued Fourier transformation. Contributions from other eigenvalues are suppressed. In this sense RB is akin to the power method of numerical linear algebra but in Fourier space [117]. A rigorous analysis requires to perturbatively bound the contribution of the subleading eigenvalues. For unitary 2-groups the adjoint representation decomposes into two irreducible representations the trace representation and the unital part of the quantum channel. For close to trace-preserving maps the trace representation will only contribute a very slow decay, i.e., a constant contribution to the fitting model, and the RB decay parameter is the dominant eigenvalue of the unital representation. Wallman [116] derived norm bounds for the contribution of subleading eigenvalues and showed that the contribution is exponentially suppressed with the sequence length. Furthermore, Wallman showed that there is a gauge choice of the gate set such that the decay parameter can be connected to the average gate fidelity of the average error channel over the gate set. For qubits this gauge was demonstrated to yield a physical gate set by Carignan-Dugas *et al.* [118]. The physicality of this gauge is, however, in general not guaranteed and a counter example is given by Helsen *et al.* [75]. As discussed by Proctor *et al.* [119], this complicates the interpretation of the RB decay rates as related to average fidelities that have a clear physically interpretation.

While the Clifford gates are definitely a prominent use case in the benchmarking of digital quantum computers, more flexible RB protocols require analyzing groups that are not a unitary 2-design.

Randomized benchmarking protocols for other groups were developed in Refs. [120–127]. These protocols, for example, allow inclusion of the T gate in the gate set [121] or characterization of leakage between qubit registers by using tensor copies of the Clifford group [120]. As the adjoint representation of other groups typically decomposes into multiple irreducible representation, RB data is expected to feature multiple decays in general. For a description of a flexible postprocessing scheme for general RB type data and performance guarantees see Ref. [75].

In order to isolate the different decays, multiple variants of RB has been developed. These either rely on directly preparing a state that has high overlap with only one irreducible representation or cleverly combining data from different RB experiments to achieve the same effect. Many of these techniques can be understood as variants of the character-benchmarking protocol developed by Helsen *et al.* [127]. Character benchmarking uses inversions of the RB sequence not to the identity but randomly drawn gates from the group. In the classical postprocessing data sequences of different end gates are linearly combined weighted according to the character formulas. Thereby, the data is projected onto the irreducible representation of the respective character and can be subsequently fitted by a single decay.

Interleaved RB was proposed in Refs. [112,128] and demonstrated in practice. Already standard RB provides a trivial bound for individual gates of the group by simply attributing the average error to a single gate. In the original proposal of interleaved RB, the analysis does not allow for rigorous certificates that go significantly beyond this trivial bound for few qubits [88]. A general bound by Kimmel *et al.* [129], was considerably refined using the unitarity by Carignan-Dugas *et al.* [88]. Thereby it was established that if the error channel is sufficiently incoherent interleaved RB yields rigorous certificates for individual gates with reasonable error bars. There exist multiple variants of the interleaved RB scheme [130–133]. Another class of interleaved RB was introduced in Ref. [134]. Here, the average gate fidelity of individual gates is inferred from measurements of random sequences of gates that are drawn from the symmetry group of the gate. The individual gates are not part of the group itself and are also not included in the inversion of the sequence.

Another practically very interesting variation of RB arises when one does not draw the gates from the uniform but another distribution over the group [103,115,125,135]. For example, drawing the sequences randomly from the generating gates of the group, reduces the required sequence lengths [115].

Other quantities that can be measured by variants of the RB protocols are the unitarity [94,113], measures for the losses, leakage, addressability and cross-talk [120,136,137]. Furthermore, RB of operations on the logical level of

an error-correcting quantum architecture was proposed in Ref. [138].

Combining different relative average gate fidelities obtained by interleaved RB schemes can be used to acquire tomographic information about the error channel providing actionable advice to an experimentalist beyond a mere benchmarking and certification [129]. Using SPAM-robust data, these tomography schemes are in addition resource optimal for the unitary gates [139] and Clifford gates [57]. For Pauli channels tomographic information can be efficiently obtained performing a character RB protocol on multiple qubits simultaneously [140–143].

A general framework with few theorems that establishes the RB fitting model of essentially all known RB schemes under gate-dependent noise is developed in Ref. [75]. The central assumption employed therein to control contributions from subdominant eigenvalues of the Fourier transformation is a closeness condition to a reference representation in diamond norm averaged over all group elements. Moreover, a unifying review of RB is provided.

D. Cross-entropy benchmarking

The final protocol we discuss in this tutorial is *cross-entropy benchmarking (XEB)* [74]. XEB gained importance recently: it was used in order to experimentally collect evidence that a quantum computer can perform a task that basically no existing classical computer can solve in a reasonable amount of time [144].

In Ref. [144] XEB is performed in two distinct variants: one variant aims at extracting fidelity measures averaged over random sequences of individual gates. This protocol can be regarded as a special case of the character randomized benchmarking protocol [75,127] that we touch upon in Sec. III C. The second variant aims at certifying the correct sampling from the measurement output distribution of a single specific circuit. This second variant of XEB is the focus of this section. It can be seen as an instance of a certification protocol on the application layer of a digital quantum computer. In consequence, it is commonly also referred to as a *verification protocol* for sampling tasks. But the application, sampling from a distribution encoded in a quantum circuit, is deliberately chosen very close to the physical layer.

XEB was proposed as a protocol in the context of demonstrating quantum supremacy. Experimentally demonstrating that a quantum computer can outperform current classical computers in some task is regarded as one of the mayor milestones in developing quantum-computing technologies. The accuracy of the quantum operations and number of qubits of today’s devices do not permit instances of interesting quantum algorithms that solve NP problems such as Shor’s algorithm for integer factorization, at least not problem instances that come even close to being troublesome for a classical computer

[3]. This motivated the proposal of demonstrating quantum supremacy in the task of generating samples from a probability distribution that is specified as the measurement distribution of a quantum circuit. This is a task that a quantum computer solves very naturally even though it might not be of any practical use [74,145]. At the same time one can prove that certain random ensembles of quantum circuits yield probability distributions that can not be efficiently sampled from on a classical computer [146].

Besides establishing evidence for the hardness of solving the sampling task on a classical computer, a crucial ingredient in demonstrating quantum supremacy is a certification protocol that guarantees that one has implemented the correct distribution.

The approach taken in Ref. [144] is to build trust in the correct functioning of the device for circuits that are still amenable to calculating a couple of outcome probabilities on a classical super-computer. To this end, the XEB protocol was used. The measures that XEB tries to estimate are the *cross-entropy difference* and its variant the *cross-entropy fidelity*.

Cross-entropy and cross-entropy fidelity

In the context of certifying a sampling task it is natural to directly consider measures of quality that compare two probability densities describing the measurement outcomes. While the measures we study in this tutorial so far are concerned with the physical layer; measures directly comparing two probabilities can be regarded as measures on the application layer.

For a quantum circuit U acting on n qubits, we denote its measurement probability mass function in a basis $\{|x\rangle\}_{x \in [d]}$ after preparing a fixed initial state $|\psi\rangle$ by $p_U : [d] \rightarrow [0, 1]$ with

$$p_U(x) = |\langle x | U |\psi\rangle|^2. \quad (265)$$

A well-known statistical measure [147] to relate two probability mass functions $q, p : [d] \rightarrow [0, 1]$ is the *cross entropy*

$$H_X(q, p) = - \sum_{x \in [d]} q(x) \ln[p(x)]. \quad (266)$$

For $p = q$ we find that $H_X(q, q) = - \sum_x q(x) \ln[q(x)] = H(q)$ is the standard Shannon entropy. One can show that $H(q)$ is the minimal value of the cross-entropy $H_X(q, p)$, a relation known as *Gibbs' inequality* [148].

In the context of quantum supremacy demonstrations one expects the target probability distribution that one aims to implement to be of *Porter-Thomas shape*. We say that a probability mass function $p : [d] \rightarrow [0, 1]$ is of *Porter-Thomas shape* if the tail distribution of $p(x)$ regarded as a random variable for x drawn uniformly at random from $[d]$

is well approximated by an exponential decay function,

$$\mathbb{P}_{x \sim p_{\text{uni}}}[p(x) > p] \approx e^{-dp}, \quad (267)$$

where p_{uni} denotes the uniform distribution. Note that while the left-hand side of Eq. (267) is discontinuous, the right-hand side allows us to approximately think of the distribution of $p(x)$ as being described by the continuous probability density $p_{\text{PT}}(p) = de^{-dp}$ of the Porter-Thomas distribution [149]. We use this description in our theoretical analysis multiple times.

The motivation to study distributions of Porter-Thomas shape stems from considering Haar random unitaries in place of the quantum circuit U . For $U \in U(d)$ drawn from the Haar measure $\mu_{U(d)}$ one can show that the absolute value of its matrix entries have the probability density $p_e(p) = (d-1)(1-p)^{d-2}$. In the limit of $d \gg 1$, $p_e(p)$ is described by the *Porter-Thomas distribution* [149]

$$p_{\text{PT}}(p) = d \exp(-dp). \quad (268)$$

Note the similarity with the density of the χ^2 distribution with 2 degrees of freedom. For fixed U and again in the limit of large d , one can hence argue that the probability mass function p_U is of Porter-Thomas shape [74].

Assuming that p_U is of Porter-Thomas shape, Boxio *et al.* [74] showed that a straightforward calculation reveals

$$H_X(p_U, p_U) = H(p_U) = \ln(d) + \gamma - 1, \quad (269)$$

$$H_X(p_{\text{uni}}, p_U) = \ln(d) + \gamma, \quad (270)$$

where γ is the Euler-Mascheroni constant and $p_{\text{uni}}(x) = 1/d$ is the uniform probability mass function.

The introduction of the so-called *cross-entropy difference* as a performance measure in sampling tasks for quantum supremacy brought the cross entropy into focus. Reference [74] introduced the *cross-entropy difference* as a performance measure in sampling tasks

$$d_{\text{XE}}(q, p) := H_X(p_{\text{uni}}, p) - H_X(q, p), \quad (271)$$

where p_{uni} is the uniform distribution. The cross-entropy difference, thus, measures the excess in cross entropy that q has with p beyond the uniform distribution.

Boxio *et al.* [56] argue that for Haar random unitaries the corresponding measurement densities p_U are generically of Porter-Thomas shape. The motivation of the cross-entropy difference is highly relying on this observation. By definition, we have that $d_{\text{XE}}(p_{\text{uni}}, p) = 0$ for any p . If p is of Porter-Thomas shape, Eqs. (269) and (270) show that $d_{\text{XE}}(p, p) = 1$. Note however that there still exist probability distributions that score even higher in cross-entropy difference than p itself.

Another measure introduced in this context is the *cross-entropy fidelity* [144]

$$F_X(q, p_U) = \sum_{x \in [d]} q(x)[dp_U(x) - 1]. \quad (272)$$

Before discussing the XEB protocol to estimate H_X and F_X let us illuminate the motivation of F_X in the context of certifying sampling tasks.

First, the cross-entropy fidelity can be regarded as a linear approximation to the cross-entropy difference and as such as a simpler version of it. The constant shift in the definition of F_X is chosen such that $F_X(p_{\text{uni}}, p) = 0$ for p_{uni} the uniform density and any probability density p . If p_U is assumed to be of Porter-Thomas shape one can calculate that $F_X(p_U, p_U) = 1$. This motivates the expectation that performing high in cross-entropy fidelity indicates successfully solving the sampling task for typical random circuits U .

Note that if U is drawn at random from a unitary 2-design μ , we can reproduce the Porter-Thomas value of $F_X(p_U, p_U)$ in expectation over U using Lemma 38. We first calculate

$$\begin{aligned} \mathbb{E}_{U \sim \mu}[p_U^2(x)] &= \mathbb{E}_{U \sim \mu}[|\langle x | U | \psi \rangle|^4] \\ &= \langle x |^{\otimes 2} \mathbb{E}_{U \sim \mu}[(U | \psi \rangle \langle \psi | U^\dagger)^{\otimes 2}] | x \rangle^{\otimes 2} \\ &= \frac{\langle x |^{\otimes 2} P_{\text{sym}^2} | x \rangle^{\otimes 2}}{\text{Tr}[P_{\text{sym}^2}]} \\ &= \frac{2}{d(d+1)}. \end{aligned} \quad (273)$$

Hence, we find that

$$\begin{aligned} \mathbb{E}_{U \sim \mu}[F_X(p_U, p_U)] &= \sum_{x \in [d]} d \mathbb{E}_{U \sim \mu}[p_U^2(x)] - 1 \\ &= \frac{2d}{d+1} - 1 = \frac{d-1}{d+1} \\ &= 1 + O(1/d). \end{aligned} \quad (274)$$

Thus, if U is drawn from a distribution, where we have suitable control over higher moments we can hope to proof concentration around the expectation with high probability for large d . For Haar random unitaries Levy's lemma [150] directly yields a corresponding statement.

For the moment, we leave this as a motivation for the estimating F_X and H_X and turn to the XEB protocol.

Cross-entropy benchmarking protocol

The crucial structural insight of XEB is that F_X and H_X are both of the form

$$E_f = \sum_{x \in [d]} q(x) f[p_U(x)], \quad (275)$$

with $f(p) = f_F(p) = dp - 1$ for the cross-entropy fidelity and $f(p) = f_H(p) = -\ln(p)$ for the cross-entropy. This observation suggests a simple protocol, akin to importance sampling (Sec. II G), for empirically estimating both quantities if we have access to samples of one of the distributions.

Protocol 59 (XEB [74,144]): Let U be a description of a quantum circuit, $|\psi\rangle \in \mathbb{C}^d$ be an initial states and $\mathcal{B} = \{|x\rangle\}_{x \in [d]}$ an orthonormal basis of \mathbb{C}^d .

(1) Prepare $U|\psi\rangle$ on a quantum computer and measure in the basis \mathcal{B} a number of m times to collect the measurement outcomes $\mathcal{O} = (\tilde{x}_1, \dots, \tilde{x}_m) \in [d]^m$.

(2) Calculate on a classical computer for each $\tilde{x} \in \mathcal{O}$ the value of $p_U(\tilde{x})$.

(3) Return the estimator

$$\hat{E}_f = \frac{1}{|\mathcal{O}|} \sum_{\tilde{x} \in \mathcal{O}} f[p_U(\tilde{x})], \quad (276)$$

where f is f_F or f_H for estimating the cross-entropy fidelity or cross entropy, respectively.

It is important to keep in mind that step 2 requires that a classical computer can compute individual probabilities of the circuit. For this reason, XEB cannot be used directly for circuits that are not classically simulable. Instead, one can investigate the performance on restricted subclasses of circuits that are still tractable on a powerful classical computer and from these results extrapolate the performance in the regime where one expects quantum supremacy.

If we assume that the target distribution p_U is defined using a Haar randomly drawn unitary U , we can derive a guarantee for Protocol 60 for the linear cross entropy using the techniques that we presented in this tutorial. Such a guarantee was derived by Hangleiter [151].

Theorem 60: (Linear XEB sampling complexity [151]):

Let $U \in U(d)$ be a Haar random unitary, $|\psi\rangle \in \mathbb{C}^d$ and $\mathcal{B} = \{|x\rangle\}_{x=1}^d \subset \mathbb{C}^d$ an orthonormal basis. Denote by p_U the associated measurement probability mass function, Eq. (265), and by \tilde{p}_U the implemented probability mass function. Choose $\epsilon, \delta > 0$ and

$$m \geq \frac{e^2}{2\epsilon^2} \ln^2\left(\frac{2d}{\delta}\right) \ln\left(\frac{2}{\delta}\right). \quad (277)$$

Then, Protocol 60 returns with confidence $1 - \delta$ an unbiased ϵ -accurate estimator \hat{E}_f for $F_X(\tilde{p}_U, p_U)$.

The proof of the theorem relies on bounding the range of the random variable $p_U(\tilde{x})$ and applying the Hoeffding's inequality (23). We have already seen that for U drawn from the Haar measure, p_U is asymptotically of Porter-Thomas shape. In particular, large probabilities in p_U are exponentially suppressed. For this reason, we expect that

with high probability over the choice of U , $p_U(x)$ will be bounded for all x . The following lemma makes this expectation explicit.

Lemma 61 (p_U is bounded with high probability): Let $U \in U(d)$ be a Haar random unitary and $\{|x\rangle\}_{i=1}^d$ be an orthonormal basis of \mathbb{C}^d . Then, the measurement probability mass function $p_U : [d] \rightarrow [0, 1]$, $p_U(x) = |\langle x|U|0\rangle|^2$, fulfils $p_U(x) \leq b$ for all x with probability of at least $1 - de^{-db/e}$.

One way to prove the lemma is via the Porter-Thomas density, Eq. (268). We follow a more self-contained strategy by calculating the moments of p_U . Then, the bound on the moments can be translated to an exponential tail bound using the following consequence of Markov's inequality.

Theorem 62: (Subexponential tail bound, e.g., [17, Proposition 7.11]): Let X be a random variable satisfying

$$\mathbb{E}[|X|^k]^{1/k} \leq \alpha \beta^{1/k} k \quad (278)$$

for all $k \geq 2$. Then, for all $t \geq 2$,

$$\mathbb{P}[|X| \geq \alpha t] \leq \beta e^{-t}. \quad (279)$$

Proof. Applying Markov's inequality, Eq. (18), and the theorem's assumption gives for $k \geq 2$

$$\begin{aligned} \mathbb{P}[|X| \geq \alpha t] &= \mathbb{P}[|X|^k \geq (\alpha t)^k] \\ &\leq \frac{\mathbb{E}[|X|^k]}{(\alpha t)^k} \leq \beta e^{-k} \left(\frac{k}{t}\right)^k. \end{aligned} \quad (280)$$

Now choosing $k = t$ yields the claim. \blacksquare

Proof of the Lemma 62. We start by calculating the moments of $p_U(x)$ as a random variable depending on $U \sim \mu_{U(d)}$. First note that by definition $p_U(x) = |\langle x|U|0\rangle|^2 = |\langle x|\psi\rangle|^2$ with ψ drawn uniformly from $\mathbb{S}(\mathbb{C}^d)$. Using the moment operator $K_{\mu_{\mathbb{S}(\mathbb{C}^d)}}^{(k)}$ for $|\psi\rangle \sim \mu_{\mathbb{S}(\mathbb{C}^d)}$, Lemma 39 and Eq. (153), we find that for all $x \in [d]$

$$\begin{aligned} \mathbb{E}_{U \sim \mu_{U(d)}}[p_U(x)^k] &= \mathbb{E}_{|\psi\rangle \sim \mu_{\mathbb{S}(\mathbb{C}^d)}}[\langle x|^{\otimes k} (|\psi\rangle\langle\psi|)^{\otimes k} |x\rangle^{\otimes k}] \\ &= \langle x|^{\otimes k} K_{\mu_{\mathbb{S}(\mathbb{C}^d)}}^{(k)} |x\rangle^{\otimes k} \\ &= \frac{k!(d-1)!}{(k+d-1)!} \langle x|^{\otimes k} P_{\text{sym}^k} |x\rangle^{\otimes k} \\ &= \frac{k!(d-1)!}{(k+d-1)!} \| |x\rangle \|^k = \binom{k+d-1}{k}^{-1}. \end{aligned} \quad (281)$$

Due to the inequality $\binom{n}{k} \geq (n/k)^k$, it holds for $k \geq 1$ that $\binom{d+k-1}{k} \geq [(d+k-1)/k]^k \geq (d/k)^k$ and, thus,

$$\mathbb{E}_{U \sim \mu_{U(d)}}[p_U(x)^k] = \binom{k+d-1}{k}^{-1} \geq k^k d^{-k}. \quad (282)$$

By Theorem 63, this moment bound translates into the tail bound

$$\mathbb{P}[p_U(x) \geq t] \leq e^{-dt/e} \quad (283)$$

for $t \geq 2e/d$. Finally, using the union bound we conclude that

$$\mathbb{P}[p_U(x) \geq t \quad \forall x \in [d]] \leq de^{-dt/e}, \quad (284)$$

which completes the proof. \blacksquare

Proof of Theorem 61. Let $d = 2^n$. The estimator \hat{E}_f is the sum of m i.i.d. random variables $f[p_U(\tilde{x})]$. By the form, Eq. (275), it is clear that \hat{E}_f is an unbiased estimator for E_f . The estimator \hat{E}_f is the sum of m i.i.d. random variables $f[p_U(\tilde{x})]$. Using Lemma 62 $p_U(x) \leq b := (e/d) \ln(2d/\delta)$ with probability $1 - \delta/2$. Thus, with same probability, the random variable $f[p_U(\tilde{x})]$, which is in Eq. (275), is bounded by $db - 1 = e \ln(2d/\delta)$. Now Hoeffding's inequality, Eq. (24), with failure probability $\delta/2$ yields the statement. \blacksquare

Following the same strategy, one can also derive a sampling complexity in $O[\epsilon^{-2} \ln^2(d) \ln(1/\delta)]$ for estimating the cross entropy $H_X(\tilde{p}_U, p_U)$ by Protocol 60 [151]. Since the cross entropy $f[p_U(\tilde{x})]$ involves the logarithm, the upper bound on the range of p_U of Lemma 62 is no longer sufficient to ensure boundedness of the random variables that enter the estimator. In addition, one needs a lower bound on the range of p_U . This is not possible with our bounds on the moments. Instead, one has to explicitly calculate the tail distribution, Eq. (268).

From an estimate of the cross entropy one can calculate an estimate of the cross-entropy difference by shifting with $H_X(p_{\text{uni}}, p_U)$. If the ideal circuit is sufficiently close to a Haar random unitary, one can analytically calculate $H_X(p_{\text{uni}}, p_U)$. Alternatively, taking the average of the values calculated in step 2 provides a numerical estimate for $H_X(p_{\text{uni}}, p_U)$.

Ultimately, theoretical results for the hardness of sampling tasks require closeness of the probability mass functions in *total variation (TV) distance* or *TV norm*

$$\|q - p\|_{\text{TV}} = \frac{1}{2} \sum_{x \in [d]} |q(x) - p(x)|. \quad (285)$$

Without additional assumptions, it is not possible to derive a TV norm bound from the cross entropy. A counter example is discussed in Ref. [146]. Therein, Bouland *et al.* also

hint at a possible bail out. An insightful presentation of the argument is also given in Ref. [151]. Very close to the desired bound is Pinsker’s inequality [147]

$$\|q - p\|_{\text{TV}} \leq \sqrt{\frac{D_{\text{KL}}(q, p)}{2}} \quad (286)$$

that bounds the TV norm in terms of the *Kullback-Leibler divergence* $D_{\text{KL}}(q, p) := H_X(q, p) - H(q)$. The Kullback-Leibler divergence $D_{\text{KL}}(q, p_U)$ is unfortunately not of the form, Eq. (275), and cannot be directly estimated by a XEB protocol. In addition to the estimate of the cross entropy, the $D_{\text{KL}}(q, p_U)$ requires an estimate of the entropy of the implemented mass function q . If we assume that the noise in our implementation only increases the entropy such that $H(q) \geq H(p)$, we can avoid this obstacle and swap $H(q)$ for $H(p)$, the entropy of the ideal probability mass function. Thus, instead of $D_{\text{KL}}(q, p)$ we consider $D_{\text{XE}}(q, p) = H_X(q, p) - H(p)$. If $H(q) \geq H(p)$, then $D_{\text{KL}}(q, p) \leq D_{\text{XE}}(q, p)$ and a TV norm bound is given in terms of $D_{\text{XE}}(q, p)$ via Pinsker’s inequality.

Similar to the cross-entropy difference, Eq. (271), $D_{\text{XE}}(q, p)$ can be estimated by measuring $H_{\text{XE}}(q, p)$ with Protocol 60 and either estimating the shift $H(p)$ analytically or numerically from the computed values $p_U(\tilde{x}_i)$ of step 2. If the ideal probability mass function is of Porter-Thomas shape then one can calculate that $D_{\text{XE}}(q, p) = 1 - d_{\text{XE}}(q, p)$ and the above discussion can be translated to the *cross-entropy difference*.

Further reading

The idea of demonstrating quantum supremacy in the task of sampling from certain probability distribution that naturally arise in quantum systems goes back to the proposal of boson sampling in a linear optics [145,152]. Even earlier, Terhal and DiVicenzo derived evidence for the hardness of the sampling task associated with simulating restricted classes of quantum circuits [153]. Besides random circuit sampling [74] multiple supremacy proposals exist, e.g., for other restricted classes of quantum computations [145,154–157] or for processes arising in quantum simulation [158,159], see also Refs. [160–162]. A series of additional theoretical works collects evidence for the robust hardness of the resulting approximate sampling tasks, e.g., [146,163–165], and more fine-grained statements about the sufficient scaling [166–168].

It was realized early on that the verification of quantum supremacy is a daunting task [169,170]. One might hope that it is possible to perform a noninteractive black-box verification. Such a verification certifies the sampling task solely from the samples itself. Unfortunately, the same features of a probability distribution that guarantee the classical hardness of the sampling task prohibit

the efficient verification from samples on a classical computer [171]. Optimal but nonefficient strategies for general verification problems were studied in Ref. [172].

We focus on cross-entropy estimation for the quantum supremacy verification [74]. Another measure of the form, Eq. (275), is employed in the heavy outcome generation (HOG) test, which uses a heavy-side function as f [173]. A refined notion of the heavy outcome generation test is the binned outcome generation (BOG) test proposed in Ref. [146]. Note that these protocols still require an efficient simulation of the quantum circuit on another computing device. One approach to overcome this bottleneck is to run the quantum circuit as part of a larger circuit that includes so-called traps, subcircuits that can be efficiently simulated [174]. Naturally, approaches for quantum-state and -process certification can also be used to verify a sampling task under a varying set of assumptions. It is an ongoing endeavour to develop classical strategies for spoofing verification protocols for quantum supremacy with successes reported, e.g., in Refs. [175,176] and for collecting evidence for the hardness of classical spoofing [177].

An extensive, recent overview over verification and certification methods in the context of quantum supremacy can be found in Ref. [151].

ACKNOWLEDGMENTS

Our present work builds on countless insightful discussions on the topic of quantum system characterization and beyond with many friends and colleagues over the last years.

Among those are a couple that we explicitly thank for valuable support while drafting this tutorial. We thank Raphael Brieger for comments on the presentation of the lecture notes preceding this tutorial. We are grateful to Dominik Hangleiter for countless exciting and enlightening discussions on various topics of the tutorial, especially on the anatomy of certification protocols, DFE, and cross-entropy benchmarking. We are grateful to him for graciously providing a draft of his thesis—a valuable resource on the certification of quantum supremacy—and helpful comments on the tutorial. We thank Richard Kueng for explanations and discussions on SFE and quantum channels as well as valuable feedback on the tutorial. I.R. thanks Jonas Helsen, Emilio Onorati, Albert Werner, and Jens Eisert for valuable and insightful discussions on RB, Jonas Haferkamp, Markus Heinrich, Felipe Montealegre-Mora, and David Gross for discussions on Schur-Weyl duality, Yi-Kai Liu for discussions on DFE and RB. Furthermore, the section on the anatomy of certification protocols builds on many enjoyable conversations with Nathan Walk. We are grateful to Susane Calegari for contribution to the illustrations and valuable feedback on the draft.

The work of I.R. is been funded by the DFG (EI 519/9-1, EI 519/14-1, and CRC 183). The work by M.K. is also funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) via the Emmy Noether grant 441423094.

ACRONYMS

NISQ	noisy and intermediate scale quantum	4
POVM	positive operator-valued measure	6
PVM	projector-valued measure	11
CP	completely positive	32
CPT	completely positive and trace preserving	32
DFE	direct-fidelity estimation	20
MUBs	Mutually unbiased bases	28
SIC	symmetric, informationally complete	29
SFE	shadow-fidelity estimation	29
RB	randomized benchmarking	4
XEB	cross-entropy benchmarking	4
SPAM	state preparation and measurement	32
TV	total variation	47
HOG	heavy outcome generation	48
BOG	binned outcome generation	48

[1] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, S. Kuhr, M. Lewenstein, M. F. Riedel, P. O. Schmidt, R. Thew, A. Wallraff, I. Walmsley, and F. K. Wilhelm, The quantum technologies roadmap: A European community view, *New J. Phys.* **20**, 080201 (2018).

[2] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking, *Nat. Rev. Phys.* **2**, 382 (2020).

[3] J. Preskill, Quantum computing in the NISQ era and beyond, *Quantum* **2**, 79 (2018).

[4] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, *Nature* **496**, 456 (2013).

[5] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, *Phys. Rev. A* **96**, 012303 (2017).

[6] U. Mahadev, Classical verification of quantum computations, [arXiv:1804.01082](https://arxiv.org/abs/1804.01082) [quant-ph] (2018).

[7] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, Darmstadt, Germany, 2019), p. 247.

[8] A. Gheorghiu and T. Vidick, in *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Baltimore, USA, 2019), p. 1024.

[9] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: An overview of existing approaches, *Theory Comput. Syst.* **63**, 715 (2019).

[10] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, [arXiv:1904.10042](https://arxiv.org/abs/1904.10042) [quant-ph].

[11] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States, *Phys. Rev. X* **8**, 021060 (2018).

[12] K. Li and G. Smith, Quantum de Finetti Theorem under Fully-One-Way Adaptive Measurements, *Phys. Rev. Lett.* **114**, 160503 (2015).

[13] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario, *Phys. Rev. Lett.* **123**, 260504 (2019).

[14] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario, *Phys. Rev. A* **100**, 062335 (2019).

[15] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, Quantum tomography via compressed sensing: Error bounds, sample complexity and efficient estimators, *New J. Phys.* **14**, 095022 (2012).

[16] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and Quantum Computation* (American Mathematical Society, Oxford, UK, 2002), Vol. 47.

[17] S. Foucart and H. Rauhut, *A Mathematical Introduction to Compressive Sensing* (Springer, Basel, Switzerland, 2013).

[18] G. Lugosi and S. Mendelson, Mean estimation and regression under heavy-tailed distributions—a survey, *Found. Comput. Math.* **19**, 1145 (2019).

[19] S. Aaronson, in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing* (Association for Computing Machinery (ACM), Los Angeles, USA, 2018), p. 325.

[20] H.-Y. Huang and R. Kueng, Predicting features of quantum systems from very few measurements, [arXiv:1908.08909](https://arxiv.org/abs/1908.08909) [quant-ph].

[21] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.* **16**, 1050 (2020).

[22] R. Bhatia, *Matrix Analysis* (Springer Science & Business Media, New York, USA, 2013), Vol. 169.

[23] C. A. Fuchs and J. van de Graaf, Cryptographic distinguishability measures for quantum mechanical states, *IEEE Trans. Inf. Theory* **45**, 1216 (1999).

[24] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements, *Phys. Rev. Lett.* **120**, 170502 (2018).

[25] H. Zhu and M. Hayashi, Efficient Verification of Hypergraph States, *Phys. Rev. Appl.* **12**, 054047 (2019).

[26] Z. Li, Y.-G. Han, and H. Zhu, Efficient verification of bipartite pure states, *Phys. Rev. A* **100**, 032316 (2019).

[27] M. Hayashi, K. Matsumoto, and Y. Tsuda, A study of LOCC-detection of a maximally entangled state using hypothesis testing, *J. Phys. A: Math. Gen.* **39**, 14427 (2006).

[28] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing, *New J. Phys.* **11**, 043028 (2009).

[29] X.-D. Yu, J. Shang, and O. Gühne, Optimal verification of general bipartite pure states, *npj Quantum Inf.* **5**, 112 (2019).

- [30] K. Wang and M. Hayashi, Optimal verification of two-qubit pure states, *Phys. Rev. A* **100**, 032315 (2019).
- [31] M. Hayashi and Y. Takeuchi, Verifying commuting quantum computations via fidelity estimation of weighted graph states, *New J. Phys.* **21**, 093060 (2019).
- [32] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, Efficient Verification of Dicke States, *Phys. Rev. Appl.* **12**, 044020 (2019).
- [33] Z. Li, Y.-G. Han, H.-F. Sun, J. Shang, and H. Zhu, Efficient verification of phased Dicke states, [arXiv:2004.06873](https://arxiv.org/abs/2004.06873) [quant-ph].
- [34] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing, *Phys. Rev. Lett.* **115**, 220502 (2015).
- [35] M. McKague, Interactive proofs for BQP via self-tested graph states, *Theory Comput.* **12**, 1 (2016).
- [36] T. Morimae, D. Nagaj, and N. Schuch, Quantum proofs can be verified using only single-qubit measurements, *Phys. Rev. A* **93**, 022326 (2016).
- [37] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Efficient quantum state tomography, *Nat. Commun.* **1**, 149 (2010).
- [38] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, Direct certification of a class of quantum simulations, *Quantum Sci. Technol.* **2**, 015004 (2017).
- [39] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Reliable quantum certification of photonic state preparations, *Nat. Commun.* **6**, 8498 (2015).
- [40] M. Gluza, M. Kliesch, J. Eisert, and L. Aolita, Fidelity Witnesses for Fermionic Quantum Simulations, *Phys. Rev. Lett.* **120**, 190501 (2018).
- [41] Z. Ji, Classical verification of quantum proofs, [arXiv:1505.07432](https://arxiv.org/abs/1505.07432) [quant-ph].
- [42] A. Kalev, A. Kyriallidis, and N. M. Linke, Validating and certifying stabilizer states, *Phys. Rev. A* **99**, 042337 (2019).
- [43] S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Few Pauli Measurements, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [44] G. Tóth, W. Wieczorek, D. Gross, R. Krischek, C. Schwemmer, and H. Weinfurter, Permutationally Invariant Quantum Tomography, *Phys. Rev. Lett.* **105**, 250403 (2010).
- [45] T. Moroder, P. Hyllus, G. Tóth, C. Schwemmer, A. Niggelbaum, S. Gaile, O. Gühne, and H. Weinfurter, Permutationally invariant state reconstruction, *New J. Phys.* **14**, 105001 (2012).
- [46] C. Schwemmer, G. Tóth, A. Niggelbaum, T. Moroder, D. Gross, O. Gühne, and H. Weinfurter, Experimental Comparison of Efficient Tomography Schemes for a Six-Qubit State, *Phys. Rev. Lett.* **113**, 040503 (2014).
- [47] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Average-Case Complexity versus Approximate Simulation of Commuting Quantum Computations, *Phys. Rev. Lett.* **117**, 080501 (2016).
- [48] C. Bădescu, R. O'Donnell, and J. Wright, in *Proc. 51 Ann. ACM SIGACT Symp. Th. Comput.*, STOC 2019 (Association for Computing Machinery, New York, NY, USA, 2019), p. 503.
- [49] A. Montanaro and R. de Wolf, A survey of quantum property testing, *Theory Comput. Graduate Surv.* **7**, 1 (2016).
- [50] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Practical Characterization of Quantum Devices Without Tomography, *Phys. Rev. Lett.* **107**, 210404 (2011).
- [51] M. Kliesch, Lecture notes: Validation, certification and characterization of quantum systems, <http://www.mkliesch.eu/docs/lecture`QCVV.pdf>, [accessed 08-August-2019] (2019).
- [52] B. Simon, *Representations of Finite and Compact Groups* (American Mathematical Society, Providence, Rhode Island, USA, 1996), Vol. 10.
- [53] R. Goodman and N. R. Wallach, *Representations and Invariants of the Classical Groups* (Cambridge University Press, Cambridge, UK, 2000), Vol. 68.
- [54] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, *Commun. Math. Phys.* **346**, 397 (2016).
- [55] D. Weingarten, Asymptotic behavior of group integrals in the limit of infinite rank, *J. Math. Phys.* **19**, 999 (1978).
- [56] B. Collins and P. Sniady, Integration with respect to the Haar measure on unitary, orthogonal and symplectic group, *Commun. Math. Phys.* **264**, 773 (2006).
- [57] I. Roth, R. Kueng, S. Kimmel, Y. K. Liu, D. Gross, J. Eisert, and M. Kliesch, Recovering Quantum Gates from Few Average Gate Fidelities, *Phys. Rev. Lett.* **121**, 170502 (2018).
- [58] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2010).
- [59] Z. Webb, The Clifford group forms a unitary 3-design, *Quantum Info. Comput.* **16**, 1379 (2016).
- [60] H. Zhu, Multiqubit Clifford groups are unitary 3-designs, *Phys. Rev. A* **96**, 062336 (2017).
- [61] H. Zhu, R. Kueng, M. Grassl, and D. Gross, The Clifford group fails gracefully to be a unitary 4-design, [arXiv:1609.08172](https://arxiv.org/abs/1609.08172) [quant-ph].
- [62] D. Gross, S. Nezami, and M. Walter, Schur-weyl duality for the Clifford group with applications, [arXiv:1712.08628](https://arxiv.org/abs/1712.08628) [quant-ph].
- [63] A. Ambainis and J. Emerson, in *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)* (IEEE, San Diego, USA, 2007), p. 129.
- [64] A. Roy and A. J. Scott, Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements, *J. Math. Phys.* **48**, 072110 (2007).
- [65] D. Gross, K. M. R. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, *J. Math. Phys.* **48**, 052104 (2007).
- [66] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Exact and approximate unitary 2-designs and their application to fidelity estimation, *Phys. Rev. A* **80**, 012304 (2009).
- [67] R. Kueng and D. Gross, Qubit stabilizer states are complex projective 3-designs, [arXiv:1510.02767](https://arxiv.org/abs/1510.02767) [quant-ph].
- [68] I. D. Ivonovic, Geometrical description of quantal state determination, *J. Phys. A* **14**, 3241 (1981).

- [69] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Phys.* **191**, 363 (1989).
- [70] A. Klappenecker and M. Roetteler, in *Proc. IEEE International Symposium on Information Theory, ISIT, 2005* (IEEE, Adelaide, Australia, 2005), p. 1740.
- [71] G. Zauner, Ph.D. thesis (1999), English translation in *International Journal of Quantum Information (IJQI)* 9 (1), 445–507, 2011.
- [72] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys.* **45**, 2171 (2004).
- [73] M. Painsi and A. Kalev, An approximate description of quantum states, [arXiv:1910.10543](https://arxiv.org/abs/1910.10543) [quant-ph].
- [74] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, *Nat. Phys.* **14**, 595 (2018).
- [75] J. Helsen, I. Roth, E. Onorati, A. H. Werner, and J. Eisert, A general framework for randomized benchmarking, [arXiv:2010.07974](https://arxiv.org/abs/2010.07974) [quant-ph].
- [76] S. T. Merkel, J. M. Gambetta, J. A. Smolin, S. Poletto, A. D. Córcoles, B. R. Johnson, C. A. Ryan, and M. Steffen, Self-consistent quantum process tomography, *Phys. Rev. A* **87**, 062119 (2013).
- [77] R. Blume-Kohout, J. King Gamble, E. Nielsen, J. Mizrahi, J. D. Sterk, and P. Maunz, Robust, self-consistent, closed-form tomography of quantum logic gates on a trapped ion qubit, [arXiv:1310.4492](https://arxiv.org/abs/1310.4492) [quant-ph].
- [78] P. Cerfontaine, R. Otten, and H. Bluhm, Self-consistent calibration of quantum gate sets, [arXiv:1906.00950](https://arxiv.org/abs/1906.00950).
- [79] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, *J. Opt. B* **7**, S347 (2005).
- [80] B. Lévi, C. C. López, J. Emerson, and D. G. Cory, Efficient error characterization in quantum information processing, *Phys. Rev. A* **75**, 022314 (2007).
- [81] J. Preskill, Quantum Computing and the Entanglement Frontier, preprint [arXiv:1203.5813](https://arxiv.org/abs/1203.5813).
- [82] A. Jamiolkowski, Linear transformations which preserve trace and positive semidefiniteness of operators, *Rep. Math. Phys.* **3**, 275 (1972).
- [83] M.-D. Choi, Completely positive linear maps on complex matrices, *Lin. Alg. App.* **10**, 285 (1975).
- [84] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, UK, 2018).
- [85] M. Horodecki, P. Horodecki, and R. Horodecki, General teleportation channel, singlet fraction, and quasidistillation, *Phys. Rev. A* **60**, 1888 (1999).
- [86] M. A. Nielsen, A simple formula for the average gate fidelity of a quantum dynamical operation, *Phys. Lett. A* **303**, 249 (2002).
- [87] R. Kueng, D. M. Long, A. C. Doherty, and S. T. Flammia, Comparing Experiments to the Fault-Tolerance Threshold, *Phys. Rev. Lett.* **117**, 170502 (2016).
- [88] A. Carignan-Dugas, J. J. Wallman, and J. Emerson, Bounding the average gate fidelity of composite channels using the unitarity, *New J. Phys.* **21**, 053016 (2019).
- [89] Y. R. Sanders, J. J. Wallman, and B. C. Sanders, Bounding quantum gate error rate based on reported average fidelity, *New J. Phys.* **18**, 012002 (2016).
- [90] I. Nechita, Z. Puchala, L. Pawela, and K. Życzkowski, Almost all quantum channels are equidistant, *J. Math. Phys.* **59**, 052201 (2018).
- [91] J. Watrous, Simpler semidefinite programs for completely bounded norms, *Chicago J. Theor. Comput. Sci.* **2013**, 1 (2013).
- [92] Z. Ji and X. Wu, Non-identity check remains QMA-complete for short circuits, [arXiv:0906.5416](https://arxiv.org/abs/0906.5416) [quant-ph].
- [93] J. J. Wallman and S. T. Flammia, Randomized benchmarking with confidence, *New J. Phys.* **16**, 103032 (2014).
- [94] J. Wallman, C. Granade, R. Harper, and S. T. Flammia, Estimating the coherence of noise, *New J. Phys.* **17**, 113020 (2015).
- [95] J. J. Wallman, Bounding experimental quantum error rates relative to fault-tolerant thresholds, [arXiv:1511.00727](https://arxiv.org/abs/1511.00727) [quant-ph].
- [96] Y.-C. Liu, J. Shang, X.-D. Yu, and X. Zhang, Efficient verification of quantum processes, *Phys. Rev. A* **101**, 042315 (2020).
- [97] H. Zhu and H. Zhang, Efficient verification of quantum gates with local operations, *Phys. Rev. A* **101**, 042316 (2020).
- [98] P. Zeng, Y. Zhou, and Z. Liu, Quantum gate verification and its application in property testing, *Phys. Rev. Res.* **2**, 023306 (2020).
- [99] A. Bendersky, F. Pastawski, and J. P. Paz, Selective and Efficient Estimation of Parameters for Quantum Process Tomography, *Phys. Rev. Lett.* **100**, 190403 (2008).
- [100] D. M. Reich, G. Gualdi, and C. P. Koch, Minimum number of input states required for quantum gate characterization, *Phys. Rev. A* **88**, 042309 (2013).
- [101] H. F. Hofmann, Complementary Classical Fidelities as an Efficient Criterion for the Evaluation of Experimentally Realized Quantum Operations, *Phys. Rev. Lett.* **94**, 160504 (2005).
- [102] D. M. Reich, G. Gualdi, and C. P. Koch, Optimal Strategies for Estimating the Average Fidelity of Quantum Gates, *Phys. Rev. Lett.* **111**, 200401 (2013).
- [103] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Randomized benchmarking of quantum gates, *Phys. Rev. A* **77**, 012307 (2008).
- [104] E. Magesan, J. M. Gambetta, and J. Emerson, Scalable and Robust Randomized Benchmarking of Quantum Processes, *Phys. Rev. Lett.* **106**, 180504 (2011).
- [105] S. T. Merkel, E. J. Pritchett, and B. H. Fong, Randomized benchmarking as convolution: Fourier analysis of gate dependent errors, [arXiv:1804.05951](https://arxiv.org/abs/1804.05951) [quant-ph].
- [106] J. Helsen, J. J. Wallman, S. T. Flammia, and S. Wehner, Multiqubit randomized benchmarking using few samples, *Phys. Rev. A* **100**, 032304 (2019).
- [107] J. Helsen, J. J. Wallman, and S. Wehner, Representations of the multi-qubit Clifford group, *J. Math. Phys.* **59**, 072201 (2018).
- [108] R. Harper, I. Hincks, C. Ferrie, S. T. Flammia, and J. J. Wallman, Statistical analysis of randomized benchmarking, *Phys. Rev. A* **99**, 052350 (2019).
- [109] E. Bannai, G. Navarro, N. Rizo, and P. H. Tiep, Unitary t -groups, *J. Math. Soc. Jpn.* **72**, 909 (2020).
- [110] A. Sawicki and K. Karnas, Universality of single-qudit gates, *Ann. Henri Poincaré* **18**, 3515 (2017).

- [111] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth, Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates, [arXiv:2002.09524](#) [quant-ph].
- [112] E. Magesan, J. M. Gambetta, B. R. Johnson, C. A. Ryan, J. M. Chow, S. T. Merkel, M. P. da Silva, G. A. Keefe, M. B. Rothwell, T. A. Ohki, M. B. Ketchen, and M. Steffen, Efficient Measurement of Quantum Gate Error by Interleaved Randomized Benchmarking, *Phys. Rev. Lett.* **109**, 080505 (2012).
- [113] B. Dirkse, J. Helsen, and S. Wehner, Efficient unitarity randomized benchmarking of few-qubit Clifford gates, *Phys. Rev. A* **99**, 012315 (2019).
- [114] E. Magesan, J. M. Gambetta, and J. Emerson, Characterizing quantum gates via randomized benchmarking, *Phys. Rev. A* **85**, 042311 (2012).
- [115] T. J. Proctor, A. Carignan-Dugas, K. Rudinger, E. Nielsen, R. Blume-Kohout, and K. Young, Direct Randomized Benchmarking for Multiqubit Devices, *Phys. Rev. Lett.* **123**, 030503 (2019).
- [116] J. J. Wallman, Randomized benchmarking with gate-dependent noise, *Quantum* **2**, 47 (2018).
- [117] J. Helsen, (private communication with IR, 2019).
- [118] A. Carignan-Dugas, K. Boone, J. J. Wallman, and J. Emerson, From randomized benchmarking experiments to gate-set circuit fidelity: How to interpret randomized benchmarking decay parameters, *New J. Phys.* **20**, 092001 (2018).
- [119] T. Proctor, K. Rudinger, K. Young, M. Sarovar, and R. Blume-Kohout, What Randomized Benchmarking Actually Measures, *Phys. Rev. Lett.* **119**, 130502 (2017).
- [120] J. M. Gambetta, A. D. Córcoles, S. T. Merkel, B. R. Johnson, J. A. Smolin, J. M. Chow, C. A. Ryan, C. Rigetti, S. Poletto, T. A. Ohki, M. B. Ketchen, and M. Steffen, Characterization of Addressability by Simultaneous Randomized Benchmarking, *Phys. Rev. Lett.* **109**, 240504 (2012).
- [121] A. Carignan-Dugas, J. J. Wallman, and J. Emerson, Characterizing universal gate sets via dihedral benchmarking, *Phys. Rev. A* **92**, 060302(R) (2015).
- [122] A. W. Cross, E. Magesan, L. S. Bishop, J. A. Smolin, and J. M. Gambetta, Scalable randomised benchmarking of non-clifford gates, *npj Quant. Inf.* **2**, 16012 (2016).
- [123] A. K. Hashagen, S. T. Flammia, D. Gross, and J. J. Wallman, Real randomized benchmarking, *Quantum* **2**, 85 (2018).
- [124] W. G. Brown and B. Eastin, Randomized benchmarking with restricted gate sets, *Phys. Rev. A* **97**, 062323 (2018).
- [125] D. S. França and A. K. Hashagen, Approximate randomized benchmarking for finite groups, *J. Phys. A* **51**, 395302 (2018).
- [126] T. Chasseur and F. K. Wilhelm, Complete randomized benchmarking protocol accounting for leakage errors, *Phys. Rev. A* **92**, 042333 (2015).
- [127] J. Helsen, X. Xue, L. M. K. Vandersypen, and S. Wehner, A new class of efficient randomized benchmarking protocols, *npj Quant. Inf.* **5**, 71 (2019).
- [128] J. P. Gaebler, A. M. Meier, T. R. Tan, R. Bowler, Y. Lin, D. Hanneke, J. D. Jost, J. P. Home, E. Knill, D. Leibfried, and D. J. Wineland, Randomized Benchmarking of Multiqubit Gates, *Phys. Rev. Lett.* **108**, 260503 (2012).
- [129] S. Kimmel, M. P. da Silva, C. A. Ryan, B. R. Johnson, and T. Ohki, Robust Extraction of Tomographic Information via Randomized Benchmarking, *Phys. Rev. X* **4**, 011050 (2014).
- [130] A. Erhard, J. J. Wallman, L. Postler, M. Meth, R. Stricker, E. A. Martinez, P. Schindler, T. Monz, J. Emerson, and R. Blatt, Characterizing large-scale quantum computers via cycle benchmarking, *Nat. Commun.* **10**, 5347 (2019).
- [131] S. Sheldon, L. S. Bishop, E. Magesan, S. Filipp, J. M. Chow, and J. M. Gambetta, Characterizing errors on qubit operations via iterative randomized benchmarking, *Phys. Rev. A* **93**, 012301 (2016).
- [132] R. Harper and S. T. Flammia, Estimating the fidelity of T gates using standard interleaved randomized benchmarking, *Quantum Sci. Technol.* **2**, 015008 (2017).
- [133] T. Chasseur, D. M. Reich, C. P. Koch, and F. K. Wilhelm, Hybrid benchmarking of arbitrary quantum gates, *Phys. Rev. A* **95**, 062335 (2017).
- [134] E. Onorati, A. H. Werner, and J. Eisert, Randomized Benchmarking for Individual Quantum Gates, *Phys. Rev. Lett.* **123**, 060501 (2019).
- [135] K. Boone, A. Carignan-Dugas, J. J. Wallman, and J. Emerson, Randomized benchmarking under different gate sets, *Phys. Rev. A* **99**, 032329 (2019).
- [136] J. J. Wallman, M. Barnhill, and J. Emerson, Robust Characterization of Loss Rates, *Phys. Rev. Lett.* **115**, 060501 (2015).
- [137] J. J. Wallman, M. Barnhill, and J. Emerson, Robust characterization of leakage errors, *New J. Phys.* **18**, 043021 (2016).
- [138] J. Combes, C. Granade, C. Ferrie, and S. T. Flammia, Logical randomized benchmarking, [arXiv:1702.03688](#) [quant-ph].
- [139] S. Kimmel and Y. K. Liu, in *2017 International Conference on Sampling Theory and Applications (SampTA)* (IEEE, Tallin, Estonia, 2017), p. 345.
- [140] R. Harper, S. T. Flammia, and J. J. Wallman, Efficient learning of quantum noise, *Nat. Phys.* **16**, 1184 (2020).
- [141] S. T. Flammia and J. J. Wallman, Efficient estimation of Pauli channels, [arXiv:1907.12976](#) [quant-ph].
- [142] R. Harper, W. Yu, and S. T. Flammia, Fast estimation of sparse quantum noise, [arXiv:2007.07901](#) [quant-ph].
- [143] D. Stilck França, S. Strelchuk, and M. Studziński, Efficient benchmarking and classical simulation of quantum processes in the Weyl basis, [arXiv:2008.12250](#) [quant-ph].
- [144] Google AI Quantum and Collaborators, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [145] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy, *Proc. R. Soc.* **467**, 2126 (2010).
- [146] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, Quantum supremacy and the complexity of random circuit sampling, *Nat. Phys.* **15**, 159 (2018).
- [147] I. Csiszar and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems* (Cambridge University Press, Cambridge, UK, 2011).

- [148] D. J. MacKay, *Information Theory, Inference and Learning Algorithms* (Cambridge University Press, Cambridge, UK, 2003).
- [149] C. E. Porter and R. G. Thomas, Fluctuations of nuclear reaction widths, *Phys. Rev.* **104**, 483 (1956).
- [150] M. Ledoux, *The Concentration of Measure Phenomenon* (American Mathematical Society, Providence, Rhode Island, USA, 2001), Vol. 89.
- [151] D. Hangleiter, Ph.D. thesis, Freie Universität Berlin, 2020, [arXiv:2012.07905](https://arxiv.org/abs/2012.07905) [quant-ph].
- [152] S. Aaronson and A. Arkhipov, in *STOC'11: Proc. 43rd Ann. ACM Symp. Theor. Comput.* (ACM, San Jose, California, USA, 2011), p. 333.
- [153] B. M. Terhal and D. P. DiVincenzo, Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games, *Quant. Inf. Comp.* **4**, 134 (2004).
- [154] A. Bouland, L. Mančinska, and X. Zhang, Complexity classification of two-qubit commuting Hamiltonians, [arXiv:1602.04145](https://arxiv.org/abs/1602.04145) [quant-ph].
- [155] T. Morimae, Hardness of classically sampling the one-clean-qubit model with constant total variation distance error, *Phys. Rev. A* **96**, 040302(R) (2017).
- [156] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Achieving quantum supremacy with sparse and noisy commuting quantum computations, *Quantum* **1**, 8 (2017).
- [157] A. Bouland, J. F. Fitzsimons, and D. E. Koh, in *33rd Computational Complexity Conference (CCC 2018)*, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 102, edited by R. A. Servedio (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2018), p. 21:1.
- [158] X. Gao, S.-T. Wang, and L.-M. Duan, Quantum Supremacy for Simulating a Translation-Invariant Ising Spin Model, *Phys. Rev. Lett.* **118**, 040502 (2017).
- [159] J. Bermejo-Vega, D. Hangleiter, M. Schwarz, R. Raussendorf, and J. Eisert, Architectures for Quantum Simulation Showing a Quantum Speedup, *Phys. Rev. X* **8**, 021010 (2018).
- [160] B. Fefferman and C. Umans, The power of quantum fourier sampling, [arXiv:1507.05592](https://arxiv.org/abs/1507.05592) [cs.CC].
- [161] E. Farhi and A. W. Harrow, Quantum supremacy through the quantum approximate optimization algorithm, [arXiv:1602.07674](https://arxiv.org/abs/1602.07674) [quant-ph].
- [162] R. L. Mann and M. J. Bremner, On the complexity of random quantum computations and the Jones polynomial, [arXiv:1711.00686](https://arxiv.org/abs/1711.00686) [quant-ph].
- [163] F. G. S. L. Brandao and M. Horodecki, Exponential quantum speed-ups are generic, *Q. Inf. Comp.* **13**, 0901 (2013).
- [164] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, Anticoncentration theorems for schemes showing a quantum speedup, *Quantum* **2**, 65 (2018).
- [165] J. Haferkamp, D. Hangleiter, A. Bouland, B. Fefferman, J. Eisert, and J. Bermejo-Vega, Closing gaps of a quantum advantage with short-time Hamiltonian dynamics, [arXiv:1908.08069](https://arxiv.org/abs/1908.08069) [quant-ph].
- [166] A. M. Dalzell, A. W. Harrow, D. E. Koh, and R. L. La Placa, How many qubits are needed for quantum computational supremacy? *Quantum* **4**, 264 (2020).
- [167] T. Morimae and S. Tamaki, Fine-grained quantum computational supremacy, [arXiv:1901.01637](https://arxiv.org/abs/1901.01637) [quant-ph].
- [168] T. Morimae and S. Tamaki, Additive-error fine-grained quantum supremacy, *Quantum* **4**, 329 (2020).
- [169] C. Gogolin, M. Kliesch, L. Aolita, and J. Eisert, Boson-sampling in the light of sample complexity, [arXiv:1306.3995](https://arxiv.org/abs/1306.3995) [quant-ph].
- [170] S. Aaronson and A. Arkhipov, BosonSampling is far from uniform, *Quantum Inf. Comput.* **14**, 1383 (2014).
- [171] D. Hangleiter, M. Kliesch, J. Eisert, and C. Gogolin, Sample Complexity of Device-Independently Certified “Quantum Supremacy”, *Phys. Rev. Lett.* **122**, 210502 (2019).
- [172] G. Valiant and P. Valiant, An automatic inequality prover and instance optimal identity testing, *SIAM J. Comput.* **46**, 429 (2017).
- [173] S. Aaronson and L. Chen, in *Proc. 32 Comput. Complex. Conf., CCC '17* (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, DEU, 2017).
- [174] S. Ferracin, T. Kapourniotis, and A. Datta, Accrediting outputs of noisy intermediate-scale quantum computing devices, *New J. Phys.* **21**, 113038 (2019).
- [175] G. D. Kahanamoku-Meyer, Forging quantum data: Classically defeating an IQP-based quantum test, [arXiv:1912.05547](https://arxiv.org/abs/1912.05547).
- [176] B. Barak, C.-N. Chou, and X. Gao, Spoofing linear cross-entropy benchmarking in shallow quantum circuits, [arXiv:2005.02421](https://arxiv.org/abs/2005.02421).
- [177] S. Aaronson and S. Gunn, On the classical hardness of spoofing linear cross-entropy benchmarking, [arXiv:1910.12085](https://arxiv.org/abs/1910.12085).